(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年6 月15 日 (15.06.2006)

PCT

(10) 国際公開番号
WO 2006/061976 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *G09C 1/00* (2006.01)
G06F 21/24 (2006.01) *G11B 20/10* (2006.01)

(21) 国際出願番号: PCT/JP2005/020968

(22) 国際出願日: 2005 年11 月15 日 (15.11.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-353637 2004 年12 月7 日 (07.12.2004) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 上田 健二朗 (UEDA, Kenjiro) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU, Katsumi) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 大石 丈於 (OISHI, Tateo) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 加藤 元樹 (KATO, Motoki) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

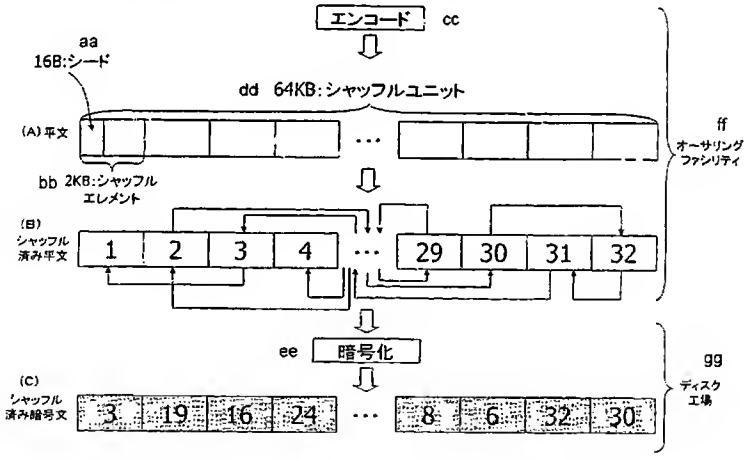
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU,

[続葉有]

(54) **Title:** INFORMATION PROCESSING DEVICE, INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING METHOD, AND COMPUTER PROGRAM

(54) **発明の名称:** 情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム



aa. 16B: SEED
(A). PLAIN TEXT
bb... 2KB: SHUFFLE ELEMENT
(B). SHUFFLED PLAIN TEXT
(C). SHUFFLED ENCRYPTED TEXT
cc.. ENCODE
dd.. 64KB: SHUFFLE UNIT
ee. ENCRYPTION
ff. AUTHORING FACILITY
gg. DISK PLANT

(57) **Abstract:** Scrambling of a content is improved, and false use of a content is excluded. Scramble rules different in contents are applied for content scrambling. For example, when shuffling is applied, various shuffle forms are defined as scramble rules. When an exclusive-OR operation is applied, the value used as exclusive-OR is defined as a scramble rule. When rotation is carried out, the amount of shift is defined as a scramble rule, When 32 shuffle elements are used for shuffling, 32! different shuffle forms, i.e., scramble rules can be defined. The value used as exclusive-OR and the amount of rotation shift can be set to various values, and many scramble rules can be set.

(57) 要約: コンテンツに対するスクランブル処理を改良し、コンテンツの不正利用の排除を可能とした構成を提供する。コンテンツのスクランブル処理としてコンテンツ毎に異なるスクランブルルールを適用する。例えばシャッフル処理を適用する場合、様々なシャッフル態様をスクランブルルールとして規定する。排他論理和処理を適用する場合、排他論理和に適

[続葉有]

WO 2006/061976 A1

ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

用する値をスクランブルルールとして規定する。また、ローテーション処理を行なう場合は、シフト量をスクランブルルールとして規定する。シャッフル処理において３２個のシャッフルエレメントを適用する場合、３２！の異なるシャッフル態様、すなわちスクランブルルールが規定可能となる。また、排他論理和に適用する値、ローテーションシフト量も様々な値に設定可能であり、多くのスクランブルルールの設定が可能となる。

明 細 書

情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

技術分野

[0001] 本発明は、情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、コンテンツ利用管理の要求される様々なコンテンツに対する高度なスクランブル処理により、不正なコンテンツ利用を排除し、厳格なコンテンツ利用管理を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ(以下、これらをコンテンツ(Content)と呼ぶ)は、記録メディア、例えば、青色レーザを適用したBlu－rayディスク、あるいはDVD(Digital Versatile Disc)、MD(Mini Disc)、CD(Compact Disc)にデジタルデータとして格納することができる。特に、青色レーザを利用したBlu－rayディスクは、高密度記録可能なディスクであり大容量の映像コンテンツなどを高画質データとして記録することができる。

[0003] これら様々な情報記録媒体(記録メディア)にデジタルコンテンツが格納され、ユーザに提供される。ユーザは、所有するPC(Personal Computer)、ディスクプレーヤ等の再生装置においてコンテンツの再生、利用を行う。

[0004] 音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

[0005] デジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをCD－R等にコピーした、いわゆる海賊版ディスクの流通

や、PC等のハードディスクに格納したコピーコンテンツの利用が蔓延しているといった問題が発生している。

[0006] DVD、あるいは近年開発が進んでいる青色レーザを利用した記録媒体等の大容量型記録媒体は、1枚の媒体に例えば映画1本～数本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

[0007] 例えば、DVDプレーヤでは、コンテンツ・スクランブルシステム(Content Scramble System)が採用されている。コンテンツ・スクランブルシステムでは、例えばDVD－ROM(Read Only Memory)にビデオデータやオーディオデータ等が暗号化されて記録されている構成において、スクランブルを解除することでコンテンツ再生を可能とするものである。

[0008] スクランブル解除処理には、ライセンスを受けたDVDプレーヤに与えられた鍵などの特定データを適用した処理を実行することが必要となる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられた鍵などの特定データを利用して、DVD－ROMに記録されたデータのスクランブル解除を行なうことにより、DVD－ROMから画像や音声を再生することができる。

[0009] 一方、ライセンスを受けていないDVDプレーヤは、スクランブル処理されたデータのスクランブル解除に適用する鍵などの特定データを有していないため、DVD－ROMに記録されたデータの再生を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD－ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

[0010] しかし、このようなコンテンツ・スクランブルシステムは、必ずしも完璧なシステムとは言いがたく、既にスクランブル解除手法が解読され解読方法がインターネット等の通

信手段を介して流通しているものも多く存在する。このように、一旦スクランブル手法が解読されてしまうと、不正なスクランブル解除処理によってコンテンツが不正に再生され、また複製されるなど、コンテンツの著作権、利用権の侵害という問題が発生する。

発明の開示

発明が解決しようとする課題

[0011] 本発明は、このような状況に鑑みてなされたものであり、著作権管理など利用管理の要求される様々なコンテンツに対するスクランブル処理を画一的な処理とすることなく、様々な異なる態様でのスクランブル処理態様を設定し、多くのスクランブル処理態様からコンテンツ毎、あるいは管理ユニット毎に設定された態様でスクランブル処理を実行する構成とすることで、厳格なコンテンツ利用管理を実現する情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

課題を解決するための手段

[0012] 本発明の第1の側面は、

情報記録媒体製造方法であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とする情報記録媒体製造方法にある。

[0013] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブルルール取得ステップは、情報記録媒体へ記録するコンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを取得するステップであることを特徴とする。

[0014] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブ

ル処理ステップは、前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なうステップであり、前記スクランブルルールは該コンテンツデータが置き換えられる位置を指し示すデータを含むことを特徴とする。

[0015] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする。

[0016] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブル処理ステップにおいて実行するスクランブル処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする。

[0017] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構成データのローテーション処理であり、前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする。

[0018] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記情報記録媒体製造方法は、さらに、前記スクランブル処理ステップの実行後、あるいは実行前に、情報記録媒体の記録コンテンツの暗号処理を実行する暗号処理ステップを有することを特徴とする。

[0019] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、前記暗号処理ステップにおいて実行する暗号処理は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理であることを特徴とする。

[0020] さらに、本発明の情報記録媒体製造方法の一実施態様において、前記スクランブル処理ステップにおいてスクランブル処理を実行する処理対象データは、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータの少なくともいずれかを含むデータとすることを特徴とする。

[0021] さらに、本発明の第2の側面は、

情報記録媒体に対するコンテンツ記録処理を実行する情報処理装置であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得し、取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理部と、

前記スクランブル処理部において生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録する記録処理部と、

を有することを特徴とする情報処理装置にある。

[0022] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、情報記録媒体へ記録するコンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを取得し、取得したスクランブルルールに従って、各コンテンツに対するスクランブル処理を実行する構成であることを特徴とする。

[0023] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なう構成であり、前記スクランブルルールは該コンテンツデータが置き換えられる位置を指し示すデータを含むことを特徴とする。

[0024] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする。

[0025] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする。

[0026] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データのローテーション処理であり、前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする。

[0027] さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、情報記録媒体の記録コンテンツの暗号処理を実行する暗号処理部を有することを特徴とする。

[0028] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、前記暗号処理部において実行する暗号処理は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理であることを特徴とする。

[0029] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、スクランブル処理対象データとして、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータとすることを特徴とする。

[0030] さらに、本発明の第3の側面は、

情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクランブル処理部を有し、

前記スクランブル処理部は、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行し、解析の結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行する構成であることを特徴とする情報処理装置にある。

[0031] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、情報記録媒体の記録コンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを取得し、取得したスクランブルルールに従って、各コンテンツに対するスクランブル解除処理を実行する構成であることを特徴とする。

[0032] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なう構成であり、前記スクランブルルールの解析の結果、取得した該コンテンツデータが置き換えられる位置を指し示す位置データを取得し、該位置データに基づいて、スクランブル解除処理を実行することを特徴とする。

[0033] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル解除処理は、コンテンツ構成データとして設定されたシャッフルエレメントのシャッフル状態を復元する処理であり、前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであり、前記スクランブル処理部は、前記スクランブルルールに基づいて、シャッフルエレメントのシャッフル状態復元処理を実行する構成であることを特徴とする。

[0034] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル解除処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、前記スクランブルルールは、前記設定値を記述したデータであり、前記スクランブル処理部は、前記スクランブルルールに基づいて、前記設定値と、コンテンツ構成データとの排他論理和演算処理を実行する構成であることを特徴とする。

[0035] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル解除処理は、コンテンツ構成データのローテーション処理であり、前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであり、前記スクランブル処理部は、前記スクランブルルールに基づいて、前記シフト量に基づくローテーション復元処理を実行する構成であることを特徴とする。

[0036] さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さ

らに、情報記録媒体の記録コンテンツの復号処理を実行する暗号処理部を有することを特徴とする。

[0037] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、前記暗号処理部において実行する復号処理は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの復号処理であることを特徴とする。

[0038] さらに、本発明の情報処理装置の一実施態様において、前記スクランブル処理部は、スクランブル解除処理対象データとして、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータを取得して処理を実行する構成であることを特徴とする。

[0039] さらに、本発明の第4の側面は、

情報記録媒体であり、

記録コンテンツ毎、または管理ユニット毎に設定されたスクランブルルールに従って、スクランブル処理の実行されたスクランブルコンテンツと、

前記スクランブルコンテンツに対して適用したスクランブルルールと、

を記録データとして格納したことを特徴とする情報記録媒体にある。

[0040] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブル処理は、前記コンテンツの少なくとも一部のデータを置き換える処理であり、前記スクランブルルールは、前記コンテンツデータの置き換える一部のデータの位置を示したデータを記録したルールであることを特徴とする。

[0041] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブルコンテンツは、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理によって生成されたスクランブルコンテンツであり、前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする。

[0042] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブルコンテンツは、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理によって生成されたスクランブルコンテンツであり、前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする。

[0043] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブルコンテンツは、コンテンツ構成データのローテーション処理によって生成されたスクランブルコンテンツであり、前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする。

[0044] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブルコンテンツは、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理によって生成されたスクランブルコンテンツであり、前記情報記録媒体は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理によって暗号化されたコンテンツを記録した構成であることを特徴とする。

[0045] さらに、本発明の情報記録媒体の一実施態様において、前記スクランブルコンテンツは、少なくとも

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかをスクランブル処理データとして含む構成であることを特徴とする。

[0046] さらに、本発明の第5の側面は、

情報記録媒体に対するコンテンツ記録処理を実行する情報処理方法であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コン

テンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とする情報処理方法にある。

[0047] さらに、本発明の第6の側面は、

情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクランブル処理ステップを有し、

前記スクランブル処理ステップは、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行するスクランブルルール解析ステップと、

前記スクランブルルール解析ステップの解析結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行するスクランブル解除ステップと、

を有することを特徴とする情報処理方法にある。

[0048] さらに、本発明の第7の側面は、

情報記録媒体に対するコンテンツ記録処理をコンピュータ上で実行させるコンピュータ・プログラムであり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0049] さらに、本発明の第8の側面は、

情報記録媒体に記録されたコンテンツの再生処理をコンピュータ上で実行させるコンピュータ・プログラムであり、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクラン

ブル処理ステップを有し、

前記スクランブル処理ステップは、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行するスクランブルルール解析ステップと、

前記スクランブルルール解析ステップの解析結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行するスクランブル解除ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

[0050] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0051] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0052] 本発明の構成によれば、著作権管理など利用管理の要求される様々なコンテンツに対するスクランブル処理を画一的な処理とすることなく、様々な異なる態様でのスクランブル処理態様を設定し、多くのスクランブル処理態様からコンテンツ毎、あるいは管理ユニット毎に選択された態様でスクランブル処理を実行する構成としたので、万が一、あるコンテンツに対応するスクランブルが不正に解析され、コンテンツが漏洩してしまった場合においても、他のスクランブル態様でスクランブル処理の施されたコンテンツはスクランブル解除が不可能であり、コンテンツの漏洩を最小限にとどめることができる。

[0053] 本発明の構成によれば、スクランブル処理として例えば、シャッフル処理、排他論

理和処理、ローテーション処理を実行し、シャッフル処理においては様々なシャッフル態様をスクランブルルールとして規定し、排他論理和処理においては排他論理和に適用する値をスクランブルルールとして規定し、ローテーション処理においてはローテーションシフト量をスクランブルルールとして規定することができる。例えば、シャッフル処理において32個のシャッフルエレメントを適用する場合、32！の異なるシャッフル態様、すなわちスクランブルルールが規定可能となる。また、排他論理和処理においては排他論理和に適用する値、ローテーション処理においてはシフト量を様々な値に設定可能であり、多くのスクランブルルールの設定が可能となり、各コンテンツに対してこれらの多くのスクランブルルールから選択したルールに基づくスクランブルを行なう構成が実現され、特定のスクランブルルールの漏洩に基づいて、多くのコンテンツが漏洩する事態を防止できる。

図面の簡単な説明

[0054] [図1]情報記録媒体の格納データ構成と、再生処理を実行する情報処理装置の構成および処理について説明する図である。

[図2]情報記録媒体の格納コンテンツに対して設定するコンテンツ管理ユニットの設定例について説明する図である。

[図3]コンテンツ管理ユニット構成およびスクランブルルールの対応例を示す図である。

[図4]コンテンツ再生を実行する情報処理装置におけるコンテンツ再生シーケンスについて説明する図である。

[図5]情報処理装置におけるコンテンツ再生に適用する鍵生成などの暗号処理の詳細について説明する図である。

[図6]コンテンツ再生を実行する情報処理装置におけるコンテンツ再生手順を説明するフローチャートを示す図である。

[図7]ライセンスエンティティ、オーサリングファシリティ、暗号化ファシリティの実行する処理について説明する図である。

[図8]スクランブル処理としてシャッフル処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図9]スクランブル処理としてシャッフル処理を実行した場合のスクランブルルールについて説明する図である。

[図10]コンテンツ暗号化を、6KBアラインドユニットを単位として実行した場合の暗号処理の詳細について説明する図である。

[図11]AES_ECBCモードを適用した暗号処理の詳細について説明する図である。

[図12]コンテンツ暗号化を、2KBユーザセクタデータを単位として実行した場合の暗号処理の詳細について説明する図である。

[図13]コンテンツ暗号化を実行する際に適用する補助ファイルについて説明する図である。

[図14]コンテンツ暗号化を実行する際に適用する補助ファイルのシンタックスを示す図である。

[図15]暗号化ファシリティにおいてスクランブル処理を実行する場合のライセンスエンティティ、オーサリングファシリティ、暗号化ファシリティの実行する処理について説明する図である。

[図16]暗号化ファシリティにおいてスクランブル処理を実行する場合、スクランブル処理としてシャッフル処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図17]MPEG2トランスポートストリームデータの構成について説明する図である。

[図18]MPEG2トランスポートストリームデータを構成するソースパケットおよびヘッダのシンタックスを示す図である。

[図19]MPEG2トランスポートストリームデータを構成するトランスポートパケットのシンタックスを示す図である。

[図20]スクランブル処理として排他論理和(EXOR)処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図21]スクランブル処理として排他論理和(EXOR)処理を実行した場合のスクランブルルールについて説明する図である。

[図22]MPEGデータを構成する例えばIピクチャの位置を取得するために適用可能なEPマップについて説明する図である。

[図23]MPEGデータを構成する例えばIピクチャの位置を取得するために適用可能なEPマップについて説明する図である。

[図24]スクランブル処理としての排他論理和(EXOR)処理をIピクチャのスライスに対して実行する場合の処理例について説明する図である。

[図25]スクランブル処理としての排他論理和(EXOR)処理をシーケンスヘッダに対して実行する場合の処理例について説明する図である。

[図26]暗号化ファシリティにおいてスクランブル処理を実行する場合において、スクランブル処理として排他論理和(EXOR)処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図27]スクランブル処理としてローテーション処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図28]スクランブル処理としてローテーション処理を実行した場合のスクランブルルールについて説明する図である。

[図29]暗号化ファシリティにおいてスクランブル処理を実行する場合において、スクランブル処理としてローテーション処理を実行した場合のコンテンツデータの変遷について説明する図である。

[図30]情報記録媒体に対する情報の記録または再生処理を実行する情報処理装置の構成例について説明する図である。

発明を実施するための最良の形態

[0055] 以下、図面を参照しながら本発明の情報処理装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムの詳細について説明する。なお、説明は、以下の記載項目に従って行う。

1. 情報記録媒体の格納データおよび再生処理
2. 情報記録媒体に対するコンテンツ記録処理の詳細
(2－1)シャッフル処理
(2－2)排他論理和演算(EXOR)処理
(2－3)ローテーション処理
3. 情報処理装置の構成例

[0056] [1. 情報記録媒体の格納データおよび再生処理]

まず、情報記録媒体の格納データおよび情報処理装置(再生装置)によるコンテンツ再生処理について説明する。図1に、本発明の処理の適用可能なコンテンツの格納された情報記録媒体100および情報処理装置(再生装置)150の構成を示す。ここでは、コンテンツ格納済みディスクとしてのROMディスクの情報格納例を示す。情報処理装置(再生装置)150は、例えばPC、あるいは再生専用装置など、様々な情報処理装置であり、情報記録媒体100からのデータ読み取り処理を実行するドライブ120を有する。

[0057] 情報記録媒体100としてのROMディスクは、例えば、Blu-rayディスク、DVDなどの情報記録媒体であり、正当なコンテンツ著作権、あるいは頒布権を持ついわゆるコンテンツ権利者の許可の下にディスク製造工場において製造された正当なコンテンツを格納した情報記録媒体である。なお、以下の実施例では、情報記録媒体の例としてディスク型の媒体を例として説明するが、本発明は様々な態様の情報記録媒体を用いた構成において適用可能である。

[0058] 図1に示すように、情報記録媒体100には、スクランブル処理および暗号化処理の施された暗号化コンテンツ111と、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックとしてのMKB(Media Key Block)112、情報記録媒体個別、あるいは所定枚数単位の情報記録媒体毎の識別情報として設定されるボリュームID113、コンテンツのコピー・再生制御情報としてのCCI(Copy Control Information)等を含む使用許諾情報114、コンテンツ復号処理に適用するタイトル鍵を生成するために必要とする情報としての記録シード(REC SEED)等から構成されるタイトル鍵データ115、さらに、情報記録媒体100に格納されたコンテンツ毎、あるいは管理ユニット毎にどのような態様のスクランブル処理が施されているかの情報を格納したスクランブルルール116が格納されている。

以下、これらの各種情報の概要について説明する。

[0059] (1)暗号化コンテンツ111

情報記録媒体100には、様々なコンテンツが格納される。例えば高精細動画像デ

ータであるHD(High Definition)ムービーコンテンツなどの動画コンテンツのAV(Audio Visual)ストリームや特定の規格で規定された形式のゲームプログラム、画像ファイル、音声データ、テキストデータなどからなるコンテンツである。これらのコンテンツは、特定のAVフォーマット規格データであり、特定のAVデータフォーマットに従って格納される。具体的には、例えばBlu－rayディスクROM規格データとして、Blu－rayディスクROM規格フォーマットに従って格納される。これらをメインコンテンツと呼ぶ。

[0060] さらに、例えばサービスデータとしてのゲームプログラムや、画像ファイル、音声データ、テキストデータなどがサブコンテンツとして格納される場合もある。サブコンテンツは、特定のAVデータフォーマットに従わないデータフォーマットを持つデータである。すなわち、Blu－rayディスクROM規格外データとして、Blu－rayディスクROM規格フォーマットに従わない任意のフォーマットで格納可能である。これらをサブコンテンツと呼ぶ。

[0061] メインコンテンツ、サブコンテンツとともに、コンテンツの種類としては、音楽データ、動画、静止画等の画像データ、ゲームプログラム、WEBコンテンツなど、様々なコンテンツが含まれ、これらのコンテンツには、情報記録媒体100からのデータのみによって利用可能なコンテンツ情報と、情報記録媒体100からのデータと、ネットワーク接続されたサーバから提供されるデータとを併せて利用可能となるコンテンツ情報など、様々な態様の情報が含まれる。情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵(タイトル鍵)が割り当てられ暗号化されて格納される。1つのタイトル鍵を割り当てる単位をコンテンツ管理ユニット(CPSユニット)と呼ぶ。

[0062] (2)MKB

MKB(Media Key Block)112は、ブロードキャストエンクリプション方式の一態様として知られる木構造の鍵配信方式に基づいて生成される暗号鍵ブロックである。MKB111は有効なライセンスを持つユーザの情報処理装置に格納されたデバイス鍵に基づく処理(復号)によってのみ、コンテンツの復号に必要なキーであるメディア鍵(Km)を取得することを可能とした鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式によって、ユーザデバイス(情報処理装置)が有効なライセン

スを持つ場合にのみ、鍵取得を可能としたものであり、無効化(リボーク処理)されたユーザデバイスの鍵(メディア鍵)取得を阻止可能としたものである。管理センタはMKBに格納する鍵情報の変更により、特定のユーザデバイスに格納されたデバイス鍵では復号できない、すなわちコンテンツ復号に必要なメディア鍵を取得できない構成を持つMKBを生成することができる。従って、任意タイミングで不正デバイスを排除(リボーク)して、有効なライセンスを持つデバイスに対してのみ復号可能な暗号化コンテンツを提供することが可能となる。コンテンツの復号処理については後述する。

[0063] (3)ボリュームID

ボリュームIDは、情報記録媒体個別、あるいは所定枚数単位の情報記録媒体毎の識別情報として設定されるIDである。このボリュームIDは、コンテンツの復号に適用するタイトル鍵の生成情報として利用される。これらの処理については後述する。

[0064] (4)使用許諾情報

使用許諾情報には、例えばコピー・再生制御情報(CCI)が含まれる。すなわち、情報記録媒体100に格納された暗号化コンテンツ111に対応する利用制御のためのコピー制限情報や、再生制限情報である。このコピー・再生制御情報(CCI)は、コンテンツ管理ユニットとして設定されるCPSユニット個別の情報として設定される場合や、複数のCPSユニットに対応して設定される場合など、様々な設定が可能である。この情報の詳細については後段で説明する。

[0065] (5)タイトル鍵データ

前述したように各コンテンツまたは複数コンテンツの集合は、コンテンツの利用管理のため、各々、個別の暗号鍵(タイトル鍵)を適用した暗号化がなされて情報記録媒体100に格納される。すなわち、コンテンツを構成するAV(Audio Visual)ストリーム、音楽データ、動画、静止画等の画像データ、ゲームプログラム、WEBコンテンツなどは、コンテンツ利用の管理単位としてのユニットに区分され、区分されたユニット毎に異なるタイトル鍵を生成して、復号処理を行なうことが必要となる。このタイトル鍵を生成するための情報がタイトル鍵データであり、例えばコンテンツの一部データなどによって構成される記録シードが利用される。

[0066] タイトル鍵データ115を適用した所定の暗号鍵生成シーケンスに従って、各ユニット

対応のタイトル鍵が生成され、コンテンツの復号が実行される。

[0067] (6)スクランブルルール

前述したように、情報記録媒体100に格納されるコンテンツは、暗号化処理が施され、さらにスクランブル処理がなされている。スクランブル処理は、情報記録媒体100に格納されるコンテンツ毎、あるいはコンテンツ管理ユニット(CPSユニット)毎に異なる態様で実行されている。従って、コンテンツ再生を行なう際には、再生対象のコンテンツに施されているスクランブル処理情報を取得し、実行されているスクランブル処理に対応するスクランブル解除処理を行なうことが必要となる。スクランブルルール116は、情報記録媒体100に格納されたコンテンツ毎、あるいはコンテンツ管理ユニット(CPSユニット)毎のスクランブル態様の情報を記録したデータである。このスクランブルルールは、ライセンスを有する情報処理装置においてのみ解読可能なデータとして情報記録媒体に記録される。例えばセキュアコード、例えばJavaセキュアコードを適用したデータとして記録され、再生装置において設定されるJavaバーチャルマシン内でのセキュアコード解読処理によってのみ解読される。

[0068] 図1には、情報記録媒体100に格納されたコンテンツの再生処理を実行する情報処理装置150の構成の概略を示している。情報処理装置は、情報岐路めく媒体の格納データの読み取り処理を実行するドライブ120を有する。ドライブ120によって読み取られたデータは、暗号化コンテンツの復号処理およびデコード(例えばMPEGデコード)処理を実行する再生処理実行LSI151に入力される。

[0069] 再生処理実行LSI151は、暗号化コンテンツの復号処理を実行する復号処理部152と、デコード(例えばMPEGデコード)処理を実行するデコード処理部153を有する。復号処理部152では、メモリ155に格納されたデバイス鍵と、情報記録媒体120からの読み取りデータとに基づいてタイトル鍵を生成し、暗号化コンテンツ111の復号処理を実行する。

[0070] 復号されたコンテンツはスクランブル処理が実行されている。このスクランブル解除を実行するのが、スクランブル解除実行部154である。復号コンテンツはスクランブル解除実行部154において、スクランブルルール115に基づいて決定されるスクランブル解除処理を実行した後、スクランブル解除データを再度、再生処理実行LSI151

に入力し、デコード処理部153において、デコード処理が実行されて出力、再生される。情報処理装置150におけるコンテンツの復号、スクランブル解除処理シーケンスの詳細については後段で説明する。

[0071] 次に、図2以下を参照して、情報記録媒体に格納されたコンテンツを区分して、区分コンテンツ毎に異なる利用制御を実現するコンテンツ管理構成について説明する。

[0072] 前述したように、情報記録媒体に格納されるコンテンツは、区分コンテンツ毎の異なる利用制御を実現するため、区分コンテンツ毎に異なる鍵(タイトル鍵)が割り当てられ暗号化処理がなされ、さらにスクランブル処理がなされて格納される。1つのタイトル鍵を割り当てる単位をコンテンツ管理ユニット(CPSユニット)と呼ぶ。

[0073] それぞれのタイトル鍵を適用して各ユニットに属するコンテンツを暗号化し、コンテンツ利用に際しては、各ユニットに割り当てられた鍵(タイトル鍵)を取得し、さらにスクランブルルールに対応するスクランブル解除を実行して再生を行う。各タイトル鍵は、個別に管理することが可能であり、例えばあるユニットAに対して割り当てるタイトル鍵は、情報記録媒体から取得可能な鍵として設定する。また、ユニットBに対して割り当てるタイトル鍵は、ネットワーク接続されるサーバにアクセスし、ユーザが所定の手続きを実行したことを条件として取得することができる鍵とするなど、各ユニット対応の鍵の取得、管理構成は、各タイトル鍵に独立した態様とすることが可能である。

[0074] 1つの鍵を割り当てる単位、すなわち、コンテンツ管理ユニット(CPSユニット)の設定態様について、図2を参照して説明する。

[0075] 図2に示すように、コンテンツは、(A)タイトル210、(B)ムービーオブジェクト220、(C)プレイリスト230、(D)クリップ240の階層構成を有し、再生アプリケーションによってアクセスされるインデックスファイルとしてのタイトルが指定されると、タイトルに関連付けられた再生プログラムが指定され、指定された再生プログラムのプログラム情報に従ってコンテンツの再生順等を規定したプレイリストが選択され、プレイリストに規定されたクリップ情報によって、コンテンツ実データとしてのAVストリームあるいはコマンドが読み出されて、AVストリームの再生、コマンドの実行処理が行われる。

[0076] 図2には、2つのCPSユニットを示している。これらは、情報記録媒体に格納された

コンテンツの一部を構成している。CPSユニット1，271、CPSユニット2，272の各々は、アプリケーションインデックスとしてのタイトルと、再生プログラムファイルとしてのムービーオブジェクトと、プレイリストと、コンテンツ実データとしてのAVストリームファイルを含むクリップを含むユニットとして設定されたCPSユニットである。

[0077] コンテンツ管理ユニット(CPSユニット)1，271には、タイトル1，211とタイトル2，212、再生プログラム221，222、プレイリスト231，232、クリップ241、クリップ242が含まれ、これらの2つのクリップ241，242に含まれるコンテンツの実データであるAVストリームデータファイル261，262がコンテンツ管理ユニット(CPSユニット)1，271に対応付けて設定される暗号鍵であるタイトル鍵:Ku1を適用して暗号化される。

[0078] コンテンツ管理ユニット(CPSユニット)2，272には、タイトル3，213、再生プログラム224、プレイリスト233、クリップ243が含まれ、クリップ243に含まれるコンテンツの実データであるAVストリームデータファイル263がコンテンツ管理ユニット(CPSユニット)2，272に対応付けて設定される暗号鍵であるタイトル鍵:Ku2を適用して暗号化される。

[0079] 例えば、ユーザがコンテンツ管理ユニット1，271に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット(CPSユニット)1，271に対応付けて設定された暗号鍵としてのタイトル鍵:Ku1を取得して復号処理を実行することが必要であり、復号処理を実行後、アプリケーションプログラムを実行してコンテンツ再生を行なうことができる。コンテンツ管理ユニット2，272に対応するアプリケーションファイルまたはコンテンツ再生処理を実行するためには、コンテンツ管理ユニット(CPSユニット)2，272に対応付けて設定された暗号鍵としてのタイトル鍵:Ku2を取得して復号処理を実行することが必要となる。

[0080] スクランブル処理についても、同様であり、コンテンツ管理ユニット毎に異なるスクランブル処理が実行されて情報記録媒体に格納される。CPSユニット1，271に対しては、スクランブルルール＃1を適用したスクランブル処理、CPSユニット2，272に対しては、スクランブルルール＃1を適用したスクランブル処理を施すなどである。コンテンツ再生時のスクランブル解除に際しては、各スクランブルルールに対応したスクランブル解除処理を実行することが必要となる。なお、スクランブルルールは、CPSユニ

ットに含まれるコンテンツ毎に変更するなどの態様とすることも可能である。

[0081] 図3は、CPSユニット単位で、異なるスクランブルルールを適用した場合の各コンテンツとCPSユニットとスクランブルルールとの対応を示すテーブルである。図3に示すように、アプリケーション層のインデックスまたはアプリケーションファイル、またはデータグループに対応するコンテンツ管理ユニット(CPSユニット)と、スクランブルルールとが対応づけられている。

[0082] コンテンツ再生処理を実行する情報処理装置150は、再生対象のコンテンツ管理ユニット(CPSユニット)を識別し、スクランブルルール116から、再生対象のコンテンツ管理ユニットに対して実行されているスクランブルルールを取得して、適用ルールに対応するスクランブル解除処理を実行して、スクランブルの解除を実行する。

[0083] 本発明の構成では、情報記録媒体に格納されているコンテンツに適用されているスクランブル処理は同一ではなく、個々のコンテンツ管理ユニット(CPSユニット)あるいはコンテンツ毎に異なる態様であり、再生処理においては、各コンテンツ管理ユニット(CPSユニット)あるいはコンテンツに対して適用されているスクランブルルールに対応したスクランブル解除処理を実行することが必要となる。

[0084] 次に、図4を参照して、上述したCPSユニット単位の暗号化およびスクランブル処理がなされた暗号化コンテンツおよび各種の鍵生成情報、スクランブルルールを格納した情報記録媒体からコンテンツを取得して再生処理を実行する情報処理装置におけるコンテンツ再生処理の詳細について説明する。

[0085] 図4に示すように、情報処理装置150において実行するコンテンツ再生処理には、暗号化コンテンツの復号処理とスクランブル解除処理の2つの処理を含む。

[0086] 情報処理装置150は、情報記録媒体100から各種の情報を読み取り、これらの読み取りデータと情報処理装置150の保有しているデバイス鍵301とを適用した鍵生成処理によって生成したタイトル鍵に基づいて暗号化コンテンツの復号処理を実行し、さらに復号コンテンツについてスクランブル解除処理を実行する。なお、この実施例ではコンテンツの復号処理の後、スクランブル解除を行なう例を示しているが、スクランブル解除の後、復号処理を行なう構成も可能であり、この処理シーケンスは、情報記録媒体に格納するコンテンツの記録処理シーケンスに依存する。

[0087] 情報処理装置150における暗号化コンテンツの復号処理およびスクランブル解除処理の詳細シーケンスについて、図4を参照して説明する。コンテンツ復号プロセスでは、まず、情報処理装置150は、メモリに格納しているデバイス鍵301を読み出す。デバイス鍵301は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。

[0088] 次に、情報処理装置150は、ステップS11において、デバイス鍵301を適用して情報記録媒体100に格納されたメディア鍵Kmを格納した暗号鍵ブロックであるMKB112の復号処理を実行して、メディア鍵Kmを取得する。

[0089] 次に、ステップS12において、ステップS11におけるMKB処理で取得したメディア鍵Kmと、情報記録媒体100から読み取ったボリュームID113とに基づく暗号処理によって、タイトル鍵生成キーKe(embedded Key)生成する。この鍵生成処理は、例えばAES暗号アルゴリズムに従った処理として実行される。

[0090] AES暗号アルゴリズムの詳細について、図5を参照して説明する。AES暗号アルゴリズムに従った処理としては、例えばAESベースのハッシュ関数[AES_H]が適用される。AESベースのハッシュ関数は、図5に示すように、AES暗号処理を適用したデータ復号処理を伴う鍵生成(Key Generation)処理実行部(AES_G)と排他的論理和部との組み合わせによって構成される。AES_G部は、さらに図5に示すようにAES復号部(AES_D)と排他的論理和部との組みによって構成される。

[0091] 図4におけるステップS12におけるタイトル鍵生成キーKe(embedded Key)の生成処理は、ステップS11におけるMKB処理で取得したメディア鍵Kmと、情報記録媒体100から読み取ったボリュームID113とを入力として、例えば図5に示すAESベースのハッシュ関数[AES_H]を適用した処理として実行される。

[0092] 次に、ステップS13において、タイトル鍵生成キーKe(embedded Key)と、情報記録媒体100から読み取った使用許諾情報114とに基づく暗号処理(AES_H)によって、コントロールキーKcを生成し、ステップS14において、コントロールキーKcと情報記録媒体100から読み取ったタイトル鍵データ115とに基づく暗号処理(AES_H)によって、タイトル鍵を生成する。

[0093] 次に、ステップS15において、情報記録媒体100から読み取った暗号化コンテンツ

に対して、タイトル鍵を適用した復号処理(例えばAES_D)が実行される。

[0094] 次に、ステップS16において、復号されたコンテンツのスクランブル解除処理を実行する。ステップS16のスクランブル解除処理は、ステップS16aのスクランブルルール取得処理と、ステップS16bのスクランブル解除処理とによって構成される。

[0095] 前述したように、コンテンツはコンテンツ管理ユニットまたはコンテンツ毎に異なるスクランブルルールが適用されたスクランブル処理が施されて情報記録媒体100に格納されている。ステップS16aのスクランブルルール取得処理は、情報記録媒体100に格納されたスクランブルルール115を取得し、再生対象のコンテンツに対応するスクランブルルールを解析する処理である。ステップS16bのスクランブル解除処理は、ステップS16aにおいて解析したスクランブルルールに対応するスクランブル解除処理を実行する。

[0096] S16aのスクランブルルール取得ステップおよびステップS16bのスクランブル解除処理は、スクランブルルールが漏洩しないようにセキュアなデータ処理として実行する必要がある。情報記録場いたに格納されるスクランブルルール115は、セキュアなJavaコードで決め区され、情報処理装置150は、Javaの実現するJavaバーチャルマシン内の処理としてステップS16aのスクランブルルール取得処理と、ステップS16bのスクランブル解除処理を実行する。

[0097] その後、スクランブル解除後のコンテンツデータしは、ステップS17において、デコード(例えばMPEGデコード)処理が実行されてコンテンツ302が出力される。

[0098] 図6に示すフローチャートを適用して情報処理装置150の実行するコンテンツ再生シーケンスについて説明する。ステップS101において、デバイス鍵を適用して情報記録媒体100に格納されたMKB112の復号処理を実行して、メディア鍵Km取得処理を実行する。ステップS102において、メディア鍵の取得に成功したと判定した場合は、ステップS103に進む。

[0099] ステップS102において、メディア鍵の取得に失敗したと判定した場合は、ステップS109に進み、再生禁止として処理を終了する。メディア鍵の取得に失敗する場合とは、情報処理装置の保持しているデバイス鍵がリボーク、すなわち不正であるとしてライセンスが認められない状態となっていることを意味する。前述したようにMKBは、

適宜更新され、有効なライセンス保持した情報処理装置の格納デバイス鍵を適用した場合にのみメディア鍵を取得することが可能な構成であり、リボークされた場合には、メディア鍵を取得することができない。

[0100] メディア鍵の取得に成功した場合は、ステップS103に進み、取得したメディア鍵Kmと、情報記録媒体100から読み取ったボリュームID113とに基づく暗号処理によって、タイトル鍵生成キーKe(embedded Key)生成する。この鍵生成処理は、前述したように例えば図5に示すAESベースのハッシュ関数[AES_H]を適用した処理として実行される。

[0101] 次に、ステップS104において、タイトル鍵生成キーKe(embedded Key)と、情報記録媒体100から読み取った使用許諾情報114とに基づく暗号処理(AES_H)によって、コントロールキーKcを生成し、ステップS105において、コントロールキーKcと情報記録媒体100から読み取ったタイトル鍵データ115とに基づく暗号処理(AES_H)によって、タイトル鍵を生成する。

[0102] 次に、ステップS106において、情報記録媒体100から読み取った暗号化コンテンツに対して、タイトル鍵を適用した復号処理(例えばAES_D)を実行し、ステップS107において、情報記録媒体100に格納されたスクランブルルール115を取得し、再生対象のコンテンツに対応するスクランブルルールを解析する処理を実行し、ステップS108において、解析したスクランブルルールに対応するスクランブル解除処理を実行する。

[0103] [2. 情報記録媒体に対するコンテンツ記録処理の詳細]

次に、情報記録媒体に対するコンテンツ記録処理の詳細について説明する。図7を参照して、コンテンツ格納情報記録媒体の製造シーケンスについて説明する。

[0104] 図7に示すように、まず、情報記録媒体に格納するコンテンツに対して、コンテンツ編集処理を実行するオーサリングファシリティ330において編集処理、すなわちステップS201におけるオーサリング処理が実行され、オーサリング済みコンテンツ332が生成される。なお、オーサリングコンテンツは、通常、MPEGエンコード等のエンコードのなされたコンテンツとして設定される。

[0105] さらに、適用するスクランブルルール331を選択して、選択したスクランブルルール

に基づいて、ステップS202においてスクランブル処理が実行される。なお、スクランブル態様には様々な態様がある。これらの具体的態様については後述する。ステップS202において、スクランブル処理がなされた後、スクランブルコンテンツは、情報記録媒体製造処理を実行するディスク工場としての暗号化ファシリティ370に渡される。

[0106] 暗号化ファシリティ370では、ステップS203において、スクランブルコンテンツに対する暗号化処理を実行する。ライセンスエンティティ350は、前述した暗号鍵ブロックとしてのMKBの管理を実行し、コンテンツ暗号化処理を実行する暗号化ファシリティ370にメディア鍵Kmを提供して、暗号化ファシリティ370は、メディア鍵を適用した処理を実行してコンテンツの暗号化を実行する。暗号化プロセスの詳細については後述する。

[0107] ステップS203における暗号化処理によって生成した暗号化コンテンツ371と、オーサリングファシリティ330において適用したスクランブルルール331とが、暗号化ファシリティ370において、情報記録媒体100に書き込まれて情報記録媒体100が製造される。

[0108] 以下、スクランブル処理の例として、

(2－1)シャッフル処理

(2－2)排他論理和演算(EXOR)処理

(2－3)ローテーション処理

の3種類のスクランブル処理について、順次説明する。

[0109] [(2－1)シャッフル処理]

図8は、図7において説明した記録データの生成処理をコンテンツデータの変化として示した図であり、適用するスクランブル処理としてシャッフル処理を適用した場合の処理例を示している。シャッフル処理をスクランブル処理として適用する場合、様々な異なるシャッフル態様がスクランブルルール毎に設定される。すなわち、

スクランブルルール＃1:シャッフル態様1

スクランブルルール＃2:シャッフル態様2

スクランブルルール＃3:シャッフル態様3

: : :

スクランブルルール＃n:シャッフル態様n

のように多数のシャッフル態様が設定され、各コンテンツあるいはコンテンツ管理ユニット(CPSユニット)毎にいずれかのスクランブルルール＃x(シャッフル態様x)が適用されてスクランブル処理が実行されることになる。

[0110] 図8には、上段から、(A)シャッフル処理前の平文、シャッフル処理後の平文、(C)シャッフル済み暗号文を示している。図8(A)に示すように、MPEGエンコード等のエンコードのなされたコンテンツ、すなわち情報記録媒体に記録するAVストリーム等のコンテンツは先頭から64KBずつに分割され、64KB毎にシャッフルユニットとして設定される。64KBシャッフルユニットは、32個の2KBシャッフルエレメントによって構成される。

[0111] スクランブル処理としてのシャッフル処理は、2KBシャッフルエレメントの入れ替え(シャッフル)処理として実行される。入れ替え態様としてのシャッフル態様がスクランブルルールである。図9を参照してスクランブルルール(シャッフル態様)について説明する。図9(A)は、1つのスクランブルルール(シャッフル態様)の例を示している。

[0112] 図9(A)に示すスクランブルルール(シャッフル態様)は、図8に示す2KBシャッフルエレメント1～32のシャッフルによる並び替え順(並び替え位置)を示している。すなわちシャッフル後は、第1番目のシャッフルエレメントとして、シャッフル前の第3番目のシャッフルエレメントを設定し、シャッフル後の第2番目のシャッフルエレメントとして、シャッフル前の第19番目のシャッフルエレメントを設定、以下、同様に、16, 24, 26・・・のにシャッフルエレメントを並び替えるシャッフル処理を示しているスクランブルルールである。

[0113] 図9(B1)がシャッフル前の2KBシャッフルエレメント1～32の設定シーケンスであり、(B2)が、(A)に示すスクランブルルール(シャッフル態様)を適用したスクランブル処理によって生成されるシャッフル後の2KBシャッフルエレメント1～32の設定シーケンスである。

[0114] スクランブルルール(シャッフル態様)は、前述したように、コンテンツ、あるいはコンテンツ管理ユニット(CPSユニット)毎に異なるルールとして設定可能である。情報記

録媒体に複数のコンテンツあるいはコンテンツ管理ユニット(CPSユニット)が記録されている場合、各コンテンツあるいはコンテンツ管理ユニット(CPSユニット)に対応して適用されているスクランブルルール、すなわち、例えば図9(A)に示すスクランブルルールがそれぞれ、図1を参照して説明したスクランブルルール116として記録されている。再生処理を実行する情報処理装置は、再生対象コンテンツに対応するスクランブルルールを読み出して、スクランブル解除処理を実行する。

[0115] 図8、図9に示す例では、32個のシャッフルユニットを適用したシャッフルをスクランブル処理として実行した例である。この場合、シャッフル態様は32！種類の設定が可能であり、スクランブルルールとして32！のルールが設定可能となる。コンテンツ、あるいはコンテンツ管理ユニット(CPSユニット)毎にこれらの32！のいずれかのルールを適用してスクランブル処理が実行可能となる。従って、ある1つのコンテンツに対応して設定されたスクランブルルールが漏洩した場合であっても、その他のコンテンツに適用されているスクランブルルールが同一のスクランブルルールである確率はきわめて低いものとなり、漏洩したスクランブルルールに基づいて、他のコンテンツのスクランブル解除を行なうことはほぼ不可能となり、コンテンツの不正取得、利用を防止することができる。

[0116] なお、情報記録媒体に記録されるスクランブルルール116は、暗号化データ、例えばJavaセキュアコードを適用して記述され、正当なライセンスを持つ情報処理装置においてのみ解読可能なデータとして設定されており、不正な読み取りによるルール解読は防止された構成となっている。

[0117] なお、スクランブル処理(シャッフル処理)は、コンテンツを区分することによって設定される複数の64KBのシャッフルユニット全てを対象として実行する構成としてもよいが、コンテンツを区分することによって設定される複数の64KBのシャッフルユニットから選択された一部のユニットのみを対象としてスクランブル(シャッフル)処理を実行する構成としてもよい。

[0118] なお、上述の例において、シャッフルユニットは64KBとして設定した例を示しているが、データサイズはこれに限定されるものではない。ただし、情報処理装置におけるコンテンツ再生処理においてドライブのデータ読み取り単位として設定されるECC

ブロックのサイズである64KBとシャッフルユニットサイズを同一サイズとすることで、1度のデータ読み取りによってシャッフルユニットを読み取ることが可能となる。従って、シャッフルユニットを64KBとして設定することで、再生処理の際にドライブにおいて実行するデータ取得処理とシャッフル解除処理を一連の処理として実行することができ、効率的な処理が実現される。また、図17を用いて後述するように、論理的な単位としては192byte単位であるトランスポートパケットを用いて記録されるため、かかる単位で処理を行っても良いし、更にこのトランスポートパケットの一部のみを対象としてシャッフル処理を行なっても良いことは言うまでも無い。また、ダミーデータを挿入しておいて、図9に示すスクランブルルールでダミーデータを除去するように並びかえても良い。

[0119] また、シャッフルエレメントのサイズ＝2KBは、ブルーレイ(Blu－ray)ディスクのユーザセクタデータと同一サイズである。6KB単位で設定されるアラインドユニット(Aligned Unit)において、図8に示すように先頭16バイトのみが非暗号化データ(平文)として設定される。各アラインドユニット(6KB)の先頭部には、再生処理タイミング情報としてのタイムスタンプが設定される。

[0120] 後述するコンテンツ暗号化処理において、6KB単位の暗号化処理を実行した場合、2KB単位のシャッフルを実行することで、各アラインドユニット(6KB)の2番目と3番目のユーザセクタデータのいずれかにタイムスタンプ情報が含まれる場合が多くなるが、これらの情報は暗号化されることになる。このように多くのタイムスタンプ情報が暗号化されることで、正当な復号処理、スクランブル解除処理を実行しない限りタイムスタンプ情報に基づく再生シーケンスの取得は不可能となる。

[0121] 図8(A),(B)に示すように、例えば図9に示すスクランブルルールを適用したスクランブル処理(シャッフル処理)は、オーサリングファシリティにおいて実行され、シャッフル後のデータが、暗号化ファシリティとしてのディスク工場に渡されて暗号化処理が実行され、図8(C)に示すシャッフル済み暗号文が生成される。

[0122] 暗号化処理の態様としては、例えば、6KBのアラインドユニット(6KB)を暗号化処理単位とした設定と、2KBのユーザセクタデータを暗号化処理単位とした設定とがあり、以下、これらのそれぞれの暗号化処理態様について説明する。

[0123] まず、6KBのアラインドユニット(6KB)を暗号化処理単位とした設定における暗号化処理について、図10を参照して説明する。

[0124] 図10(A)は、シャッフル済み平文を6KB単位のアラインドユニット(Aligcd Unit)として設定したデータ構成を示している。各6KBアラインドユニットは、図10(B)に示すように3個の2KBのユーザセクタデータの集合として設定されている。

[0125] 暗号化処理は、3個の2KBのユーザセクタデータからなる6KBアラインドユニットを処理単位として、AES_ECBC、すなわちAES暗号化のCBC(Cipher Block Chaining)モードを適用して実行される。暗号処理に適用する鍵は、6KBアラインドユニットの先頭16B非暗号化部401から取得するブロック鍵生成データ(128bits)と、前述したタイトル鍵(128bits)とに基づくAES暗号化および配置論理和演算によるAES鍵生成処理によって生成するブロック鍵(128bits)である。ブロック鍵は、6KBアラインドユニットの先頭16B非暗号化部401から取得するブロック鍵生成データを適用して生成されるので、各6KBアラインドユニット毎に異なる鍵として設定される。

[0126] AES_ECBCモードの暗号処理について、図11を参照して説明する。図11(A)は、図10(B)と同様の3個の2KBユーザセクタデータからなる6KBアラインドユニットを示し、図11(B)は、16B非暗号化部401とその他の暗号化部分402を示している。

[0127] 暗号化部分402は、図11(C)に示すようにそれぞれ16Bの平文ユニットに区分される。先頭の16バイト平文ユニットは、初期値(IV)と排他論理和(EXOR)され、さらにAES暗号化処理がなされて出力され、16バイト暗号文が設定される。さらに、この16バイト暗号文は、次の16バイト平文ユニットと排他論理和(EXOR)されAES暗号化がなされて、16バイトの暗号文ユニットが生成される。さらに、この16バイト暗号文ユニットが次の16バイト平文ユニットと排他論理和(EXOR)される。以下同様の処理が繰り返され、図11(D)に示す暗号文ユニット配列が生成される。なお、AES暗号化の際の鍵は、図10において説明したブロック鍵が適用される。また、初期値(IV)は、暗号化ファシリティ及び再生装置間で共有される予め定められた128ビット値が適用される。

[0128] このようにして、図10(C)に示す16B非暗号化部401と、その他の6128Bの暗号

化部分402とからなる1つの6KBアラインドユニットの暗号化データが生成される。

[0129] 次に、図12を参照して、2KBのユーザセクタデータを暗号化処理単位とした設定における暗号化処理について説明する。図12(A)は、シャッフル済み平文を2KBのユーザセクタデータとした設定を示している。

[0130] 暗号化処理は、1個の2KBのユーザセクタデータを処理単位として、AES_ECBC、すなわち図11を参照して説明したAES暗号化のCBC(Cipher Block Chaining)モードを適用して実行される。暗号処理に適用する鍵は、2KBユーザセクタデータの先頭16B非暗号化部411から取得するブロック鍵生成データ(128bits)と、前述したタイトル鍵(128bits)とに基づくAES暗号化および配置論理和演算によるAES鍵生成処理によって生成するブロック鍵(128bits)である。ブロック鍵は、2KBユーザセクタデータの先頭16B非暗号化部411から取得するブロック鍵生成データを適用して生成されるので、各2KBユーザセクタデータ毎に異なる鍵として設定される。

[0131] AES_ECBCモードの暗号処理については、図11を参照して説明したとおりであり、暗号処理の結果として、図12(B)に示す16B非暗号化部411と、その他の2032Bの暗号化部分412とからなる1つの2KBユーザセクタデータの暗号化データが生成される。

[0132] 図12を参照して説明した2KBユーザセクタデータ単位の暗号処理を実行する場合、CBCモードの連鎖は、2KBごとに完結する構成となる。先に、図8他を参照して説明したようにシャッフルエレメントは2KBに設定されている。従って、各シャッフルエレメント毎にAES_ECBCモードの連鎖関係は完結することになる。従って、2KB単位の暗号化を行なう構成では、暗号化処理と、スクランブル処理(シャッフル処理)の処理順番を変更しても得られる結果は同一となり、スクランブル処理と、暗号化処理のプロセス順を任意に設定できるというメリットがある。これは、データ記録処理、データ再生処理のいずれにも共通するメリットである。

[0133] データ記録に際しての暗号化処理の処理態様を決定するために暗号化プロセスを実行するディスク工場等の暗号化ファシリティにおいて適用する補助ファイル(MSTBL.DAT)のデータ構成を図13に示し、この補助ファイルのシンタックスを図14に

示す。

[0134] 補助ファイルは、[UD_START_Location]～[MKB_Location]まで、記録データの種類および位置情報が記述され、その後、各セクタ毎の暗号化処理をフラグ[Encryption_Flag]に基づいて実行する設定となっている。なお、カクアラインドユニット毎のデータタイプとして、第1へ第3セクタの区別と、AVストリームデータ以外の例えばJavaコードなどのデータとが判別可能な設定となり、これらのデータ種別に基づく暗号化処理態様の変更も可能な構成となっている。

[0135] 各データの意味は、図14に示すように、以下の意味を持つ。

UD_START_Location：各LayerのUser Data (Data Zone)の開始点のPhysical Sector Number。

UD_END_Location：各LayerのUser Data (Data Zone)の終了点のPhysical Sector Number。

CHT_Location：CHTの開始点のPhysical Sector Number。

CHT_Offset：CHTの開始点とHash Value (Mastering Facilityが埋めるデータ)の直前までのバイト数。

Content_Cert_Location：Content Certificateの開始点のPhysical Sector Number。

Content_Cert_Offset：Content Certificateの開始点とContent ID (Mastering Facilityが埋めるデータ)の直前までのバイト数。

UK_Inf_Location：タイトル鍵ファイルの開始点のPhysical Sector Number。そのLayerにUnit_Key.infが記録されない場合は、0000000016を記述。

UK_Inf_Offset：Unit_Key.infの開始点とEncrypted Unit Key for CPS Unit#1の直前までのバイト数。そのLayerにUnit_Key.infが記録されない場合は、0000000016を記述。

Num_of_UK：Disc全体のUnit Keyの数(＝CPS Unitの数)。

MKB_Location：MKBの開始点のPhysical Sector Number。そのLayerにMKB_Certが記録されない場合は、0000000016を記述。

N：Layer i のLogical Sector数。

Encryption_Flag：暗号化するかしないかのFlag。

Data_Type：SectorのTypeを示すFlag。

CPS_Unit_No：CPS Unit Number。

Clip_AV_File_No：クリップファイル番号。CHT作成のために使う情報。

Last_Sector_of_Clip：（Layerに関わらず）各クリップの最終Sectorを示すフラグ。

Last_Sector_of_Layer：各Layerでの各クリップの最終Sectorを示すフラグ。

[0136] 先に図7以下を参照して説明した例では、スクランブル処理をオーサリングファシリティが実行する処理例を説明したが、次に、図15を参照して、スクランブル処理と暗号化処理の2つの処理をディスク工場（暗号化ファシリティ）において実行する例について説明する。

[0137] 図15に示すように、まず、情報記録媒体に格納するコンテンツに対して、コンテンツ編集処理を実行するオーサリングファシリティ430において編集処理、すなわちステップS271におけるオーサリング処理が実行され、オーサリング済みコンテンツ332が生成される。なお、オーサリングコンテンツは、通常、MPEGエンコード等のエンコードのなされたコンテンツとして設定される。

[0138] オーサリングコンテンツは、スクランブル処理を実行することなく、暗号化ファシリティ（ディスク工場）470に渡される。暗号化ファシリティ（ディスク工場）470は、適用するスクランブルルール451を選択して、選択したスクランブルルールに基づいて、ステップS272においてスクランブル処理を実行する。ステップS272において、スクランブル処理がなされた後、ステップS273において、スクランブルコンテンツに対する暗号化処理を実行する。ライセンスエンティティ450は、前述した暗号鍵ブロックとしてのMKBの管理を実行し、コンテンツ暗号化処理を実行する暗号化ファシリティ470にメディア鍵Kmを提供して、暗号化ファシリティ470は、メディア鍵を適用した処理を実行してタイトル鍵を生成し、さらに先に図10、図12を参照して説明した手順に従って、ブロック鍵の生成、コンテンツ暗号化処理を実行する。

[0139] ステップS273における暗号化処理によって生成した暗号化コンテンツ452と、スクランブルルール451とが、暗号化ファシリティ470において、情報記録媒体100に書き込まれて情報記録媒体100が製造される。

[0140] 図16は、図15において説明した記録データの生成処理をコンテンツデータの変化

として示した図であり、スクランブル処理としてシャッフル処理を適用した場合の処理例を示している。上段から、(A)シャッフル処理前の平文、シャッフル処理後の平文、(C)シャッフル済み暗号文を示している。図15(A)は、オーサリングファシリティの生成するデータであり、MPEGエンコード等のエンコードのなされたコンテンツ、すなわち情報記録媒体に記録するAVストリーム等のコンテンツである。

[0141] 図15(B)は、シャッフル処理後の平文を示している。コンテンツは、先頭から64KBずつに分割され、64KB毎にシャッフルユニットとして設定され、32個の2KBシャッフルエレメントのシャッフルが実行される。その後、暗号化処理が実行されて、図15(C)に示すシャッフル後暗号文が生成される。本処理例では、図15(B)(C)のデータ生成を暗号化ファシリティとしてのディスク工場が実行する。

[0142] なお、暗号化処理は、先に、図10～図12を参照して説明したとど羽陽の処理、すなわち、6KBアラインドユニットを暗号化処理単位とした設定と、2KBユーザセクタデータを暗号化処理単位とした設定が可能である。2KBユーザセクタデータを暗号化処理単位とした設定においては、スクランブル処理と暗号化処理の前後関係を入れ替えても結果は同じとなり、任意の順序での処理とすることができる。

[0143] 図7以下を参照して説明したように、本発明の情報記録媒体製造処理は、情報記録媒体へ記録するコンテンツに適用するスクランブルルールを選択するスクランブルルール選択処理と、選択したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理と、生成したスクランブルコンテンツと、該コンテンツに対して選択適用したスクランブルルールを情報記録媒体に記録する処理とを実行するものである。スクランブルルール選択処理では、情報記録媒体へ記録するコンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを選択する処理を実行する。

[0144] また、スクランブル処理は、上述したコンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理の他、排他論理和演算処理、ローテーション処理などがある。以下、これらの処理について説明する。

[0145] [(2－2)排他論理和演算(EXOR)処理]

次に、スクランブル処理として、排他論理和演算(EXOR)処理を適用した処理例に

ついて説明する。まず、この処理例の説明の前に、情報記録媒体に記録するAVストリームのエンコードデータ、すなわちMPEG2トランスポートストリームデータのデータ構成について説明する。

[0146] 図17は、MPEG2トランスポートストリームデータのデータ構成を示す図である。MPEG2トランスポートストリームデータは図17(A)に示すように、6KBアラインドユニットの連結データとして設定される。各6KBアラインドユニットは、図17(B)に示すように、192ビットのソースパケット32個から構成される。なお、192ビットのソースパケット32個は、3個の2KBユーザセクタデータに相当する。

[0147] 各192バイトソースパケットは、図17(C)に示すように、4ビットTP_extraヘッダと、188ビットトランスポートパケットによって構成される。図18(A)にソースパケットのシンタックス、図18(B)にTP_extraヘッダのシンタックス、図19にトランスポートパケットのシンタックスを示す。

[0148] スクランブル処理として、排他論理和演算(EXOR)処理を適用する処理は、平文のトランスポートストリームデータ上の所定箇所のnビット(たとえば32ビット)データに所定のnビット(32ビット)値を排他論理和(EXOR)する処理として実行される。所定のnビット(32ビット)値はスクランブルルールによって規定される値である。

[0149] 図20を参照して、オーサリングファシリティにおいてスクランブル処理(EXOR処理)を実行する場合のコンテンツ(MPEG2ストリームデータ)の変遷について説明する。

[0150] 図20(A)は、MPEG2トランスポートストリームの構成データである。オーサリングファシリティでは、スクランブルルールに基づいて決定される値(32ビット値Vi)を取得し、予め定められたMPEG2トランスポートストリームの構成データ位置にスクランブルルールから取得したnビット(32ビット)値を排他論理和(EXOR)する処理を実行して、図20(B)EXOR済み平文を生成する。

[0151] スクランブルルールは、例えば、図21に示すルールとして設定される。図21には、V(1)～V(n)の32ビットデータが格納され、これらの各V(i)値もしくはこれらを元に計算される値が、MPEG2トランスポートストリームから選択されたn箇所の32ビットデータに順次、排他論理和(EXOR)が施されてデータの書き換えが実行され、スクランブル処理が行なわれることになる。なお、1つの値、例えばV(1)のみをスクランブル

ルールとして設定し、MPEG2トランスポートストリームから選択されたn箇所の32ビットデータに順次、同一の値V(1)もしくはこれを元に計算される値を排他論理和(EXOR)する構成としてもよい。

[0152] スクランブル処理として、排他論理和(EXOR)を施す場合は、情報記録媒体に記録されるスクランブルルールは、図21に示すルール、すなわち排他論理和(EXOR)演算の実行値もしくは実行値の元になる値が記録されることになる。再生処理におけるスクランブル解除の際には、この値もしくはこの値を元に計算される値を再度、所定位置のデータと排他論理和(EXOR)することで、オリジナルデータを復元することが可能となる。

[0153] 図20に戻り、オーサリングファシリティにおいてスクランブル処理(EXOR処理)を実行する場合のコンテンツ(MPEG2ストリームデータ)の変遷についての説明を続ける。オーサリングファシリティでは、例えば図21に示すスクランブルルールを適用して排他論理和(EXOR)演算処理を実行し、図20(B)に示すEXOR済み平文を生成し、このデータを暗号化ファシリティとしてのディスク工場に提供する。

[0154] 暗号化ファシリティとしてのディスク工場は、この受領データに対して、暗号化処理を実行して、図20(C)に示すEXOR済み暗号文を生成する。暗号化処理は、先に、図10～図12を参照して説明したAES_ECBCモードを適用した処理が適用される。

[0155] このように、排他論理和演算(EXOR)の施されたデータをデコードしても正しいデータは取得できない。正しいデータを取得するためには、排他論理和(EXOR)に適用された所定のnビット(32ビット)値を、所定箇所に再度、排他論理和(EXOR)して、オリジナルのトランスポートストリームデータを復元するというスクランブル解除処理が必要となる。所定のnビット(32ビット)値はスクランブルルールによって規定されており、正当な手続きの下でのスクランブルルール解析を行うことが必要となる。

[0156] スクランブル処理として、排他論理和演算(EXOR)処理を適用する場合、排他論理和演算(EXOR)処理を適用する対象データの選択構成として、

(a)所定のパターンでデータ内容に無関係で排他論理和演算(EXOR)処理を施す。

(b)特定の選択箇所のみに排他論理和演算(EXOR)処理を施す。

これら(a), (b)のいずれかの処理が可能である。

[0157] さらに、上記(b)特定の選択箇所のみに排他論理和演算(EXOR)処理を施す場合には、

(b1)Iピクチャのスライスを符号化したVLC(可変長ランレングス符号化データ)の一部

(b2)シーケンスヘッダの一部もしくは全て

(b3)TSパケット内のPID

これら3箇所のいずれかを排他論理和演算(EXOR)適用位置として選択可能である。各設定例について説明する。

[0158] (b1)Iピクチャのスライスを符号化したVLC(可変長ランレングス符号化データ)の一部

MPEG2エンコードデータは、I, P, Bピクチャから構成されるGOP(Group of Pictures)データによって構成される。Iピクチャは、基本となる画像データであり、P, Bピクチャは、それぞれIピクチャ等からの差分データ等によって構成されるデータであり、Iピクチャの構成がくずれるとGOPに含まれるフレームデータの再現(デコード)は困難となる。

[0159] またIピクチャのスライスを符号化したVLCは、これら基幹データとしてのIピクチャのランレングス符号化データであり、このVLCに対して所定のnビット(32ビット)値を適用した排他論理和演算(EXOR)を施した場合、排他論理和演算(EXOR)処理データのデコードによってオリジナルデータの再現は不可能となり、効果的なスクランブルが実現される。

[0160] なお、データ内容に無関係で排他論理和演算(EXOR)をする場合でもトランスポートストリームの大部分がVLCデータなので、高い確率でデータを効果的にスクランブルすることが出来る。すなわち、処理データを普通に再生しても正しい映像が出ない。

[0161] なお、Iピクチャの場所は、クリップインフォメーションに含まれるEPマップ(EP_map)によって求めることが出来る。図22に示すように、EPマップ(EP_map)501は、

クリップインフォメーションに含まれるデータである。

[0162] EPマップに基づくIピクチャ位置の検出について、図23参照して説明する。図23(A)はクリップAVストリームを示し、各矩形は192ビットソースパケットを示している。各ソースパケットにはタイムスタンプが設定され再生処理時間が規定されている。

[0163] 図23(B)に、ソースパケットNo.(X1)の詳細構成を示す。1つのソースパケットは、TP_extraヘッダとトランスポートパケットとによって構成され、トランスポートパケットには、各種のヘッダ情報と、MPEG2実体データとしてのI－PICH～のデータによって構成される。

[0164] 図23(C)に示すクリップインフォメーションには、前述したようにEPマップが含まれる。EPマップには、図に示すように、[PTS_EP start]、[SPN_EP start]、[I_end_position_offset]の各データが含まれる。各データの意味は、以下の通りである。

PTS_EP_start:シーケンスヘッダを含むsource packetに対応するタイムスタンプ。

SPN_EP_start:シーケンスヘッダを含むsource packetの先頭アドレス。

I_end_position_offset:シーケンスヘッダを含むsource packetから、Iピクチャの終わりを含むsource packetのオフセット

これらのデータ関係を示すのが図23(D)である。

[0165] すなわち、図23(B)に示すように、ソースパケットに含まれるデータの構成が規定されており、図23(C)に示す[PTS_EP start]、[SPN_EP start]、[I_end_position_offset]の各データをEPマップから求めることで、これらのデータに基づいて、ソースパケット中のIピクチャ位置が求められることになる。

[0166] データ記録時、データ再生時には、このEPマップ情報からIピクチャ位置を求めて、所定のnビット(32ビット)値を適用した排他論理和演算(EXOR)を施すことになる。

[0167] なお、このようにEPマップを適用することなく、排他論理和演算(EXOR)すべき場所全ての論理ブロックアドレス(Logical Block Address)を記述したテーブルを用意し、このテーブルに基づいてスクランブル位置を求める構成としてもよい。この場合は、このテーブルもスクランブルルールとして情報記録媒体に記録する。再生処理に際し

てスクランブル解除を実行する場合は、このテーブルと、図22に示した排他論理和値とからなるスクランブルルールに基づいて、スクランブル(EXOR)位置と値を取得してEXOR処理を実行してスクランブル解除を行なう。

[0168] Iピクチャのスライスを符号化したVLCに対して、スクランブル、すなわち排他論理和(EXOR)演算を実行する処理例について、図24を参照して説明する。図24に示すように、Iピクチャのスライスを符号化したVLCは、各スライスの先頭位置を示すスタートコードによって区分されており、オーサリングファシリティでは、スクランブルルールに基づいて決定される値(32ビット値Vi)を取得し、予め定められたMPEG2トランスポートストリームのスライス位置にスクランブルルールから取得したnビット(32ビット)値を排他論理和(EXOR)する処理を実行する。

[0169] 各スライスは、VLC符号化されているので、排他論理和(EXOR)演算により一部データの書き換えが発生すると、スライスに対応するGOP全体の復号(MPEGデコード)が不可能となる。このようにIピクチャのスライスを符号化したVLCに対して、スクランブル、すなわち排他論理和(EXOR)する処理によって効果的なスクランブルが可能となる。

[0170] (b2)シーケンスヘッダの一部もしくは全て

次に、シーケンスヘッダの一部もしくは全てを排他論理和(EXOR)演算対象データとして設定した例について説明する。

[0171] シーケンスヘッダは、GOPの先頭に付加されるヘッダである。このシーケンスヘッダの場所についても、先に説明したEPマップに基づいて算出することができる。なお、上述の場合と同様に、EPマップを適用することなく、排他論理和演算(EXOR)すべき場所全ての論理ブロックアドレス(Logical Block Address)を記述したテーブルを用意し、このテーブルに基づいてスクランブル位置を求める構成としてもよい。この場合は、このテーブルもスクランブルルールとして情報記録媒体に記録する。再生処理に際してスクランブル解除を実行する場合は、このテーブルと、図22に示した排他論理和値とからなるスクランブルルールに基づいて、スクランブル(EXOR)位置と値を取得してEXOR処理を実行してスクランブル解除を行なう。

[0172] シーケンスヘッダは、MPEGデコード処理の処理態様を決定するための情報が記

録されており、この情報なしには、正しい復号(MPEGデコード)は不可能となる。従って、このシーケンスヘッダの値を排他論理和演算(EXOR)によって書き換えることによりデータ復元を不可能にすることができ、効果的なスクランブルが実現される。

[0173] 図25にシーケンスヘッダに対して、スクランブル、すなわち排他論理和(EXOR)演算を実行した処理例を示す。図25に示すように、シーケンスヘッダを含むデータ領域について、複数の32ビット値V(i)を適用して、排他論理和(EXOR)する処理を実行する。

[0174] 排他論理和(EXOR)に適用する値は、スクランブルルールから取得する。すなわち、例えば図22に示す各々32ビットの値を規定したデータを適用する。スクランブル解除の場合もこれらのデータを取得して同一位置に、排他論理和(EXOR)する処理を実行することでオリジナルのシーケンスヘッダ情報を取得することができる。

[0175] (b3)TSパケット内のPID

次に、TSパケット内のPIDを排他論理和(EXOR)演算対象データとして設定した例について説明する。

[0176] TSパケット内のPIDは、トランスポートパケットないにある13ビットのデータである(図19参照)。このPIDデータは、トランスポートパケットに含まれるデータ内容、すなわちビデオデータであるか、オーディオデータであるか等のデータ種別を判別するためのデータであり、デコード処理には不可欠なデータとなる。このデータを排他論理和(EXOR)演算により書き換えることで、正しいデコードを不可能とすることが可能となり効果的なスクランブルが実現される。

[0177] TSパケット内のPID位置は、あらかじめ規定されており、容易に求めることが可能である。ただし、この処理例の場合も、前述の例と同様、排他論理和演算(EXOR)すべき場所全ての論理ブロックアドレス(Logical Block Address)を記述したテーブルを用意し、このテーブルに基づいてスクランブル位置を求める構成としてもよい。この場合は、このテーブルもスクランブルルールとして情報記録媒体に記録する。再生処理に際してスクランブル解除を実行する場合は、このテーブルと、図22に示した排他論理和値とからなるスクランブルルールに基づいて、スクランブル(EXOR)位置と値を取得してEXOR処理を実行してスクランブル解除を行なう。

[0178] 先に、図20を参照して説明した処理例では、スクランブル処理としての排他論理和(EXOR)演算処理をオーサリングファシリティが実行する処理例を説明したが、次に、図26を参照して、スクランブル処理としての排他論理和(EXOR)演算処理と暗号化処理の2つの処理をディスク工場(暗号化ファシリティ)において実行する例について説明する。

[0179] 図26(A)は、MPEG2トランスポートストリームの構成データである。オーサリングファシリティは、編集済みコンテンツとして、MPEG2トランスポートストリームを生成し、これを暗号化ファシリティとしてのディスク工場に提供する。

[0180] 暗号化ファシリティとしてのディスク工場は、スクランブルルールに基づいて決定される値(32ビット値Vi)を取得し、予め定められたMPEG2トランスポートストリームの構成データ位置にスクランブルルールから取得したnビット(32ビット)値を排他論理和(EXOR)する処理を実行して、図26(B)EXOR済み平文を生成する。

[0181] スクランブルルールは、例えば、図21に示すルールとして設定される。図21には、V(1)～V(n)の32ビットデータが格納され、これらの各V(i)値が、MPEG2トランスポートストリームから選択されたn箇所の32ビットデータに順次、排他論理和(EXOR)が施されてデータの書き換えが実行され、スクランブル処理が行なわれることになる。なお、1つの値、例えばV(1)のみをスクランブルルールとして設定し、MPEG2トランスポートストリームから選択されたn箇所の32ビットデータに順次、同一の値V(1)を排他論理和(EXOR)する構成としてもよい。

[0182] 暗号化ファシリティとしてのディスク工場は、さらにこのデータに対して、暗号化処理を実行して、図26(C)に示すEXOR済み暗号文を生成する。暗号化処理は、先に、図10～図12を参照して説明したAES_ECBCモードを適用した処理が適用される。

[0183] このように、排他論理和演算(EXOR)の施されたデータをデコードしても正しいデータは取得できない。正しいデータを取得するためには、排他論理和(EXOR)に適用された所定のnビット(32ビット)値を、所定箇所に再度、排他論理和(EXOR)して、オリジナルのトランスポートストリームデータを復元するというスクランブル解除処理が必要となる。所定のnビット(32ビット)値はスクランブルルールによって規定されて

おり、正当な手続きの下でのスクランブルルール解析を行うことが必要となる。

[0184] [(2－3)ローテーション処理]

次に、スクランブル処理として、ローテーション処理を適用した処理例について説明する。

[0185] スクランブル処理として、ローテーション処理を適用する処理は、平文のトランスポートストリームデータ上の所定箇所のnビット(たとえば32ビット)データを、スクランブルルールによって規定されるビット数分のローテーションを実行する処理として実行される。所定のローテーションビット数はスクランブルルールによって規定される値である。

[0186] 図27を参照して、オーサリングファシリティにおいてスクランブル処理(ローテーション処理)を実行する場合のコンテンツ(MPEG2ストリームデータ)の変遷について説明する。

[0187] 図27(A)は、MPEG2トランスポートストリームの構成データである。オーサリングファシリティでは、スクランブルルールに基づいて決定されるローテーションビット数を取得し、予め定められたMPEG2トランスポートストリームのローテーション領域611, 612の構成ビットを、スクランブルルールから取得したローテーションビット数に基づいて取得ビット数分のローテーション処理を実行して、図27(B)ローテーション済み平文を生成する。

[0188] スクランブルルールは、例えば、図28に示すルールとして設定される。図28には、V(1)～V(n)のローテーションビット数データが格納される。

このテーブルを用いて次のようにローテーション(ビット入れ替え)を行う。

ローテーション位置の1箇所目は、左にV(1)ビットシフト

ローテーション位置の2箇所目は、左にV(2)ビットシフト

ローテーション位置の3箇所目は、左にV(3)ビットシフト

・・・

ローテーション位置のn箇所目は、左にV(n)ビットシフト

[0189] スクランブル処理としてローテーション処理を実行する場合は、このテーブルがスクランブルルールとして情報記録媒体に格納される。このテーブルは、例えば暗号化を

施してディスクに記録してルールが解読されないようになされる。なお、すべてのローテーション位置に対して、同一のビット数分のローテーションを行なう構成としてもよく、この場合は、1つのシフト量[V(1)]のみをスクランブルルールとして規定すればよい。なお、例えば、32ビットのユニット内でローテーションを行う場合は、シフト量Xは、X, 32の設定で規定される。

[0190] スクランブル処理として、ローテーションを施す場合は、情報記録媒体に記録されるスクランブルルールは、図28に示すルール、すなわちローテーションのビット数データ値が記録されることになる。再生処理におけるスクランブル解除の際には、この値に基づいて、再度、逆ローテーションを実行することで、オリジナルデータを復元することが可能となる。

[0191] 図27に戻り、オーサリングファシリティにおいてスクランブル処理(ローテーション処理)を実行する場合のコンテンツ(MPEG2ストリームデータ)の変遷についての説明を続ける。オーサリングファシリティでは、例えば図28に示すスクランブルルールを適用してローテーション処理を実行する。

[0192] ローテーション位置611の32ビットデータは、本来b0～b31のシーケンスで設定されていた32ビットデータであるが、ローテーションによって[b11]が先頭にシフトされている。すなわち、11ビット左シフトが実行されている。同様に、ローテーション位置612の32ビットデータは、本来b0～b31のシーケンスで設定されていた32ビットデータであるが、ローテーションによって[b25]が先頭にシフトされている。すなわち、25ビット左シフトが実行されている。このシフト量は、スクランブルルールに基づいて決定される。オーサリングファシリティは、このようにスクランブルルールに基づくローテーション処理を実行し、図27(B)に示すローテーション済み平文を生成し、このデータを暗号化ファシリティとしてのディスク工場に提供する。

[0193] 暗号化ファシリティとしてのディスク工場は、この受領データに対して、暗号化処理を実行して、図27(C)に示すローテーション済み暗号文を生成する。暗号化処理は、先に、図10～図12を参照して説明したAES_ECBCモードを適用した処理が適用される。

[0194] このように、ローテーション処理の施されたデータをデコードしても正しいデータは

取得できない。正しいデータを取得するためには、ローテーション処理の実行位置データを、ローテーション実行ビット数分、ただしく逆ローテーションすることが必要であり、この処理によって、スクランブル解除が可能となる。ローテーションビット数はスクランブルルールによって規定されており、正当な手続きの下でのスクランブルルール解析を行うことが必要となる。

[0195] なお、スクランブル処理として、ローテーション処理を適用する場合、の適用データ位置は、前述の排他論理和演算(EXOR)処理の適用対象データ位置と同様、

(a)所定のパターンでデータ内容に無関係でローテーション処理を施す。

(b)特定の選択箇所のみにローテーション処理を施す。

これら(a), (b)のいずれかの処理が可能である。

さらに、上記(b)特定の選択箇所のみにローテーション処理を施す場合には、

(b1)Iピクチャのスライスを符号化したVLC(可変長ランレングス符号化データ)の一部

(b2)シーケンスヘッダの一部もしくは全て

(b3)TSパケット内のPID

これら3箇所のいずれかをローテーション位置として選択可能である。

[0196] 図27を参照して説明した処理例では、スクランブル処理としてのローテーション処理をオーサリングファシリティが実行する処理例を説明したが、次に、図29を参照して、スクランブル処理としてのローテーション処理と暗号化処理の2つの処理をディスク工場(暗号化ファシリティ)において実行する例について説明する。

[0197] 図29(A)は、MPEG2トランスポートストリームの構成データである。オーサリングファシリティは、編集済みコンテンツとして、MPEG2トランスポートストリームを生成し、これを暗号化ファシリティとしてのディスク工場に提供する。

[0198] 暗号化ファシリティとしてのディスク工場は、スクランブルルールに基づいて決定されるローテーションビット数を取得し、予め定められたMPEG2トランスポートストリームの構成データ位置にスクランブルルールから取得したローテーションビット数分のローテーション処理を実行して、図29(B)ローテーション済み平文を生成する。

[0199] ローテーション領域621の32ビットデータは、ローテーションによって[b11]が先頭

にシフトされている。すなわち、11ビット左シフトが実行されている。同様に、ローテーション領域622の32ビットデータは、ローテーションによって[b25]が先頭にシフトされている。すなわち、25ビット左シフトが実行されている。このシフト量は、スクランブルルールに基づいて決定される。スクランブルルールは、例えば、図28に示すルールとして設定される。暗号化ファシリティとしてのディスク工場は、さらにこのデータに対して、暗号化処理を実行して、図29(C)に示すローテーション済み暗号文を生成する。暗号化処理は、先に、図10～図12を参照して説明したAES_ECBCモードを適用した処理が適用される。

[0200] このように、ローテーションの施されたデータをデコードしても正しいデータは取得できない。正しいデータを取得するためには、ローテーション処理の実行位置データを、ローテーション実行ビット数分、ただしく逆ローテーションすることが必要であり、この処理によって、スクランブル解除が可能となる。ローテーションビット数はスクランブルルールによって規定されており、正当な手続きの下でのスクランブルルール解析を行うことが必要となる。

[0201] なお、ここまで、スクランブル処理の態様として、シャッフル処理、排他論理和(EXOR)処理、ローテーション処理の3種類を説明したが、これらのスクランブル処理は組み合わせて適用する構成としてもよい。

[0202] また、スクランブル処理の対象データとして、排他論理和(EXOR)処理と、ローテーション処理については、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータとする設定例について説明したが、シャッフル処理についても同様に、上記(1)～(3)のいずれかを含むデータを選択してシャッフルを行なう構成としてもよい。

[0203] [3. 情報処理装置の構成例]

次に、図30を参照して、上述の各種スクランブル処理を施したコンテンツの記録処理または再生処理を行う情報処理装置の構成例について説明する。

[0204] 情報処理装置800は、情報記録媒体891の駆動を行ない、データ記録再生信号の入手力を行なうドライブ890、各種プログラムに従ったデータ処理を実行するCPU870、プログラム、パラメータ等の記憶領域としてのROM860、メモリ880、デジタル信号を入出力する入出力I／F810、アナログ信号を入出力し、Λ／D，D／Λコンバータ841を持つ入出力I／F840、MPEGデータのエンコード、デコード処理を実行するMPEGコーデック830、TS（Transport Stream）・PS(Program Stream)処理を実行するTS・PS処理手段820、各種の暗号処理を実行する暗号処理手段850、スクランブル処理またはスクランブル解除処理を実行するスクランブル処理手段855を有し、バス801に各ブロックが接続されている。

[0205] まず、データ記録時の動作について説明する。記録を行うデータとしてデジタル信号入力とアナログ信号入力の2つのケースが想定される。

[0206] デジタル信号の場合、デジタル信号用入出力I／F810から入力され、CPU870、TS・PS処理手段820によって保存用のデータ形式に変換し、MPEGコーデック830によって例えばMPEG2形式へのデータ変換処理を行い、スクランブル処理手段855において、所定のスクランブルルールに従ったスクランブル処理を実行する。スクランブルルールは例えばメモリ880に格納されている。スクランブル処理の態様としては、上述したように、シャッフル処理、排他論理和（EXOR）処理、あるいはローテーション処理のいずれかを適用した処理を行なう。シャッフル処理、排他論理和（EXOR）処理、あるいはローテーション処理いずれを適用する場合においても、コンテンツまたはコンテンツ管理ユニット毎に異なるルールの適用が可能である。

[0207] なお、シャッフル処理、排他論理和（EXOR）処理、あるいはローテーション処理のいずれか1つの手法によるスクランブル処理ではなく、シャッフル処理、排他論理和（EXOR）処理、ローテーション処理を、複数組み合わせて適用したスクランブル処理を実行する構成としてもよい。

[0208] スクランブル処理が実行されたデータは、次に、暗号化処理手段850によって暗号化処理を施される。暗号化処理は、先に図10～図12を参照して説明したように、例えばΛES__ECBCモードを適用した処理として実行される。AES__ECBCモードを適用した暗号化処理単位は、2KB単位、6KB単位など、様々な設定が可能である。

暗号化処理手段850によって暗号化処理を施されたデータが情報記録媒体891に保存する。

[0209] アナログ信号の場合、入出力I/F840へ入力されたアナログ信号はA/Dコンバータ841によってデジタル信号となり、MPEGコーデック830によって記録時に使用されるコーデックへと変換される。その後、TS・PS処理手段820により、記録データの形式であるAV多重化データへ変換され、必要に応じて、スクランブル処理手段855によるスクランブル処理、暗号化処理手段850による暗号化処理が施されて、記録媒体891に保存される。

[0210] 次に、情報記録媒体からのデータ再生を行なう場合の処理について説明する。例えばMPEG－TSデータからなるAVストリームデータの再生を行う場合、ドライブ890において情報記録媒体891から読み出されたデータはコンテンツ管理ユニットとして識別されると、コンテンツ管理ユニットに対応するユニット鍵の取得処理が実行され、取得されたユニット鍵に基づいて、暗号化処理手段850で暗号を解き、その後、スクランブル解除処理が実行される。

[0211] スクランブル解除処理に際しては、スクランブルルールを情報記録媒体891から読み出して、再生対象コンテンツに適用されているスクランブルルールを解析することが必要となる。例えば、コンテンツのスクランブルが、シャッフル処理として実行されている場合は、図9(A)に示すシャッフルエレメントのシーケンスを設定したスクランブルルール、排他論理和(EXOR)であれば、図21に示す排他論理和(EXOR)の値を設定したスクランブルルール、ローテーションであれば、図28に示すローテーション(シフト)ビット数を設定したスクランブルルールを取得し、これらの取得ルールに基づいてスクランブル解除を実行する。なお、前述したように、スクランブルルールの解析およびスクランブル解除処理はセキュアなデータ処理として実行される。具体的には、例えば情報記録媒体に格納されるスクランブルルールは、Javaセキュアコードで記録され、スクランブルルール解析、スクランブル解除処理は、コンテンツ再生を実行する情報処理装置に設定されるJavaVM(バーチャルマシン)上で実行される。

[0212] スクランブル解除がなされたコンテンツデータは、次に、TS(Transport Stream)・PS(Program Stream)処理手段820によってVideo、Audio、字幕などの各データに分

けられる。さらに、MPEGコーデック830において復号されたデジタルデータは入出力I/F840内のD/Aコンバータ841によってアナログ信号に変換され出力される。またデジタル出力を行う場合、MPEG－TSデータは入出力IF810を通してデジタルデータとして出力される。この場合の出力は例えばIEEE1394やイーサネットケーブル、無線LANなどのデジタルインターフェースに対して行われる。なお、ネットワーク接続機能に対応する場合入出力IF810はネットワーク接続の機能を備える。また、再生装置内で出力先機器が受信可能な形式にデータ変換をして出力を行う場合、一旦、TS・PS処理手段820で分離したVideo、Audio、字幕などに対してMPEGコーデック830においてレート変換、コーデック変換処理を加え、TS・PS処理手段820で再度MPEG－TSやMPEG－PSなどに多重化を行ったデータをデジタル用入出力I/F810から出力する。または、CPU870を使用してMPEG以外のコーデック、多重化ファイルに変換をしてデジタル用入出力I/F810から出力することも可能である。

[0213] なお、再生処理、記録処理を実行するプログラムはROM860内に保管されており、プログラムの実行処理中は必要に応じて、パラメータ、データの保管、ワーク領域としてメモリ880を使用する。なお、図30では、データ記録、再生の可能な装置構成を示して説明したが、再生機能のみの装置、記録機能のみを有する装置も構成可能であり、これらの装置においても本発明の適用が可能である。

[0214] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

[0215] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させること

が可能である。

[0216] 例えば、プログラムは記録媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD－ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

[0217] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0218] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0219] 以上、説明したように、本発明の構成によれば、著作権管理など利用管理の要求される様々なコンテンツに対するスクランブル処理を画一的な処理とすることなく、様々な異なる態様でのスクランブル処理態様を設定し、多くのスクランブル処理態様からコンテンツ毎、あるいは管理ユニット毎に選択された態様でスクランブル処理を実行する構成としたので、万が一、あるコンテンツに対応するスクランブルが不正に解析され、コンテンツが漏洩してしまった場合においても、他のスクランブル態様でスクランブル処理の施されたコンテンツはスクランブル解除が不可能であり、コンテンツの漏洩を最小限にとどめることができる。

[0220] 本発明の構成によれば、スクランブル処理として例えば、シャッフル処理、排他論理和処理、ローテーション処理を実行し、シャッフル処理においては様々なシャッフル態様をスクランブルルールとして規定し、排他論理和処理においては排他論理和

に適用する値をスクランブルルールとして規定し、ローテーション処理においてはローテーションシフト量をスクランブルルールとして規定することができる。例えば、シャッフル処理において32個のシャッフルエレメントを適用する場合、32！の異なるシャッフル態様、すなわちスクランブルルールが規定可能となる。また、排他論理和処理においては排他論理和に適用する値、ローテーション処理においてはシフト量を様々な値に設定可能であり、多くのスクランブルルールの設定が可能となり、各コンテンツに対してこれらの多くのスクランブルルールから選択したルールに基づくスクランブルを行なう構成が実現され、特定のスクランブルルールの漏洩に基づいて、多くのコンテンツが漏洩する事態を防止できる。

請求の範囲

[1] 情報記録媒体製造方法であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とする情報記録媒体製造方法。

[2] 前記スクランブルルール取得ステップは、

情報記録媒体へ記録するコンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを取得するステップであることを特徴とする請求項1に記載の情報記録媒体製造方法。

[3] 前記スクランブル処理ステップは、

前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なうステップであり、

前記スクランブルルールは該コンテンツデータが置き換えられる位置を指し示すデータを含むことを特徴とする請求項1に記載の情報記録媒体製造方法。

[4] 前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、

前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする請求項1に記載の情報記録媒体製造方法。

[5] 前記スクランブル処理ステップにおいて実行するスクランブル処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、

前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする請求項1に記載の情報記録媒体製造方法。

[6] 前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構

成データのローテーション処理であり、

前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする請求項1に記載の情報記録媒体製造方法。

[7] 前記情報記録媒体製造方法は、さらに、

前記スクランブル処理ステップの実行後、あるいは実行前に、情報記録媒体の記録コンテンツの暗号処理を実行する暗号処理ステップを有することを特徴とする請求項1に記載の情報記録媒体製造方法。

[8] 前記スクランブル処理ステップにおいて実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、

前記暗号処理ステップにおいて実行する暗号処理は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理であることを特徴とする請求項7に記載の情報記録媒体製造方法。

[9] 前記スクランブル処理ステップにおいてスクランブル処理を実行する処理対象データは、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータとすることを特徴とする請求項1に記載の情報記録媒体製造方法。

[10] 情報記録媒体に対するコンテンツ記録処理を実行する情報処理装置であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得し、取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理部と、

前記スクランブル処理部において生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録する記録処理部と、

を有することを特徴とする情報処理装置。

[11] 前記スクランブル処理部は、

情報記録媒体へ記録するコンテンツが複数ある場合において、記録コンテンツ毎、

または管理ユニット毎に個別のスクランブルルールを取得し、取得したスクランブルルールに従って、各コンテンツに対するスクランブル処理を実行する構成であることを特徴とする請求項10に記載の情報処理装置。

[12] 前記スクランブル処理部は、

前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なう構成であり、

前記スクランブルルールは該コンテンツデータが置き換えられる位置を指し示すデータを含むことを特徴とする請求項10に記載の情報処理装置。

[13] 前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、

前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする請求項10に記載の情報処理装置。

[14] 前記スクランブル処理部において実行するスクランブル処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、

前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする請求項10に記載の情報処理装置。

[15] 前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データのローテーション処理であり、

前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする請求項10に記載の情報処理装置。

[16] 前記情報処理装置は、さらに、

情報記録媒体の記録コンテンツの暗号処理を実行する暗号処理部を有することを特徴とする請求項10に記載の情報処理装置。

[17] 前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、

前記暗号処理部において実行する暗号処理は、前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理であることを特徴とする請

求項16に記載の情報処理装置。

[18] 前記スクランブル処理部は、スクランブル処理対象データとして、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータとすることを特徴とする請求項10に記載の情報処理装置。

[19] 情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理装置であり、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクランブル処理部を有し、

前記スクランブル処理部は、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行し、解析の結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行する構成であることを特徴とする情報処理装置。

[20] 前記スクランブル処理部は、

情報記録媒体の記録コンテンツが複数ある場合において、記録コンテンツ毎、または管理ユニット毎に個別のスクランブルルールを取得し、取得したスクランブルルールに従って、各コンテンツに対するスクランブル解除処理を実行する構成であることを特徴とする請求項19に記載の情報処理装置。

[21] 前記スクランブル処理部は、

前記情報記録媒体に記録するコンテンツデータの少なくとも一部を置き換える処理を行なう構成であり、

前記スクランブルルールの解析の結果、取得した該コンテンツデータが置き換えられる位置を指し示す位置データを取得し、該位置データに基づいて、スクランブル解除処理を実行することを特徴とする請求項19に記載の情報処理装置。

[22] 前記スクランブル処理部において実行するスクランブル解除処理は、コンテンツ構

成データとして設定されたシャッフルエレメントのシャッフル状態を復元する処理であり、

前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであり、

前記スクランブル処理部は、

前記スクランブルルールに基づいて、シャッフルエレメントのシャッフル状態復元処理を実行する構成であることを特徴とする請求項19に記載の情報処理装置。

[23] 前記スクランブル処理部において実行するスクランブル解除処理は、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理であり、

前記スクランブルルールは、前記設定値を記述したデータであり、

前記スクランブル処理部は、

前記スクランブルルールに基づいて、前記設定値と、コンテンツ構成データとの排他論理和演算処理を実行する構成であることを特徴とする請求項19に記載の情報処理装置。

[24] 前記スクランブル処理部において実行するスクランブル解除処理は、コンテンツ構成データのローテーション処理であり、

前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであり、

前記スクランブル処理部は、

前記スクランブルルールに基づいて、前記シフト量に基づくローテーション復元処理を実行する構成であることを特徴とする請求項19に記載の情報処理装置。

[25] 前記情報処理装置は、さらに、

情報記録媒体の記録コンテンツの復号処理を実行する暗号処理部を有することを特徴とする請求項19に記載の情報処理装置。

[26] 前記スクランブル処理部において実行するスクランブル処理は、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理であり、

前記暗号処理部において実行する復号処理は、前記シャッフルエレメントと同一サ

イズのデータを単位として実行するCBCモードの復号処理であることを特徴とする請求項25に記載の情報処理装置。

[27] 前記スクランブル処理部は、スクランブル解除処理対象データとして、

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかを含むデータを取得して処理を実行する構成であることを特徴とする請求項19に記載の情報処理装置。

[28] 情報記録媒体であり、

記録コンテンツ毎、または管理ユニット毎に設定されたスクランブルルールに従って、スクランブル処理の実行されたスクランブルコンテンツと、

前記スクランブルコンテンツに対して適用したスクランブルルールと、

を記録データとして格納したことを特徴とする情報記録媒体。

[29] 前記スクランブル処理は、前記コンテンツの少なくとも一部のデータを置き換える処理であり、

前記スクランブルルールは、前記コンテンツデータの置き換える一部のデータの位置を示したデータを記録したルールであることを特徴とする請求項28に記載の情報記録媒体。

[30] 前記スクランブルコンテンツは、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理によって生成されたスクランブルコンテンツであり、

前記スクランブルルールは、前記シャッフルエレメントのシャッフル態様を記述したデータであることを特徴とする請求項28に記載の情報記録媒体。

[31] 前記スクランブルコンテンツは、予め設定された設定値もしくは該設定値に基づいて算出される値と、コンテンツ構成データとの排他論理和演算処理によって生成されたスクランブルコンテンツであり、

前記スクランブルルールは、前記設定値を記述したデータであることを特徴とする請求項28に記載の情報記録媒体。

[32] 前記スクランブルコンテンツは、コンテンツ構成データのローテーション処理によっ

て生成されたスクランブルコンテンツであり、

前記スクランブルルールは、ローテーションにおけるシフト量を記述したデータであることを特徴とする請求項28に記載の情報記録媒体。

[33] 前記スクランブルコンテンツは、コンテンツ構成データとして設定されるシャッフルエレメントのシャッフル処理によって生成されたスクランブルコンテンツであり、

前記情報記録媒体は、

前記シャッフルエレメントと同一サイズのデータを単位として実行するCBCモードの暗号処理によって暗号化されたコンテンツを記録した構成であることを特徴とする請求項28に記載の情報記録媒体。

[34] 前記スクランブルコンテンツは、少なくとも

(1)MPEGエンコードデータに含まれるIピクチャスライス符号化データの一部

(2)シーケンスヘッダの一部

(3)トランスポートストリームパケット内のデータ種別情報を記録したPIDデータ

の少なくともいずれかをスクランブル処理データとして含む構成であることを特徴とする請求項28に記載の情報記録媒体。

[35] 情報記録媒体に対するコンテンツ記録処理を実行する情報処理方法であり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とする情報処理方法。

[36] 情報記録媒体に記録されたコンテンツの再生処理を実行する情報処理方法であり

、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクランブル処理ステップを有し、

前記スクランブル処理ステップは、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行するスクランブルルール解析ステップと、

前記スクランブルルール解析ステップの解析結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行するスクランブル解除ステップと、

を有することを特徴とする情報処理方法。

[37] 情報記録媒体に対するコンテンツ記録処理をコンピュータ上で実行させるコンピュータ・プログラムであり、

情報記録媒体へ記録するコンテンツに適用するスクランブルルールを取得するスクランブルルール取得ステップと、

前記スクランブルルール取得ステップにおいて取得したスクランブルルールに従って、コンテンツに対するスクランブル処理を実行するスクランブル処理ステップと、

前記スクランブル処理ステップにおいて生成したスクランブルコンテンツと、該コンテンツに対して適用したスクランブルルールを情報記録媒体に記録するステップと、

を有することを特徴とするコンピュータ・プログラム。

[38] 情報記録媒体に記録されたコンテンツの再生処理をコンピュータ上で実行させるコンピュータ・プログラムであり、

情報記録媒体に記録されたコンテンツのスクランブル解除処理を実行するスクランブル処理ステップを有し、

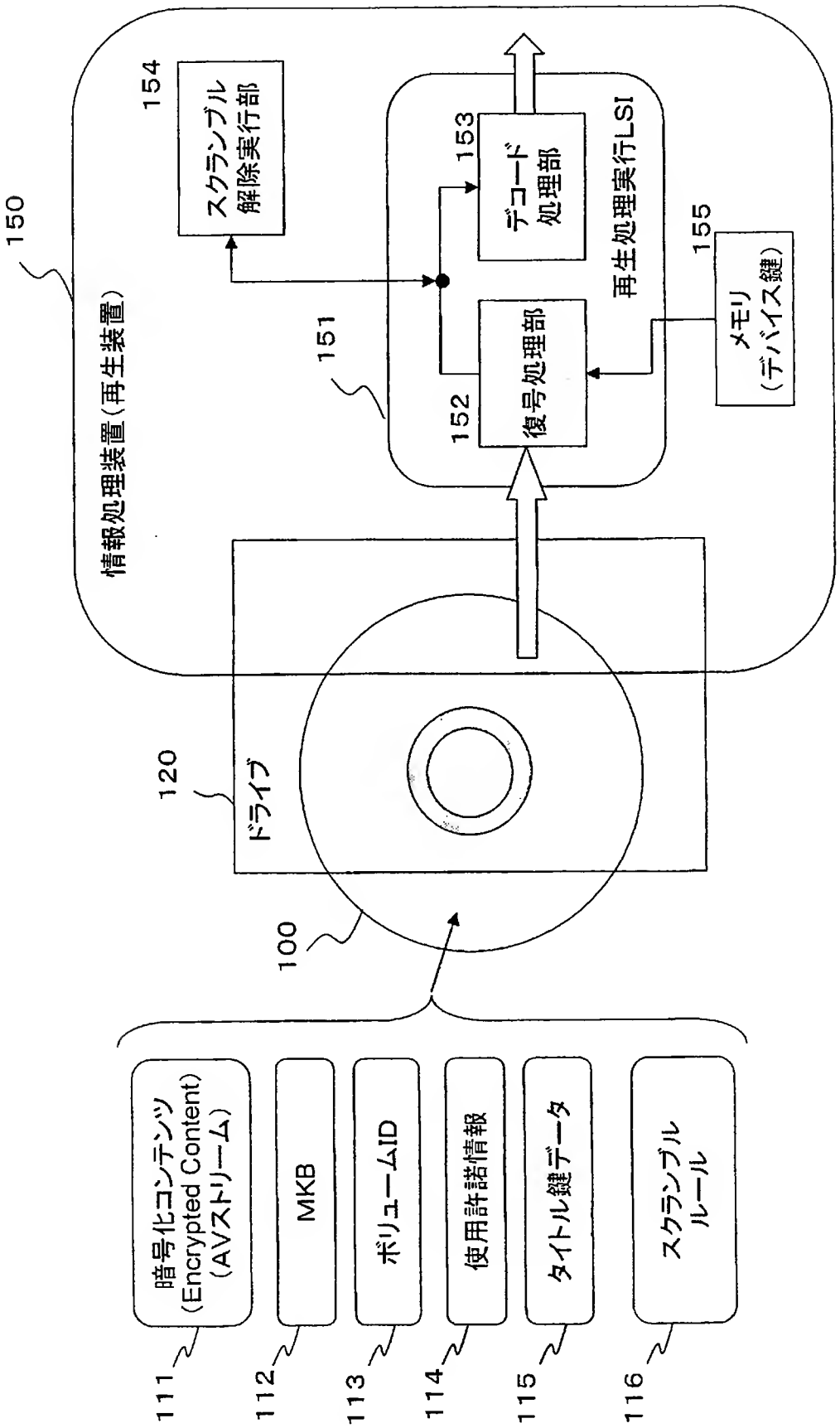
前記スクランブル処理ステップは、

前記情報記録媒体に格納されたコンテンツに対応するスクランブル処理情報としてのスクランブルルールの解析を実行するスクランブルルール解析ステップと、

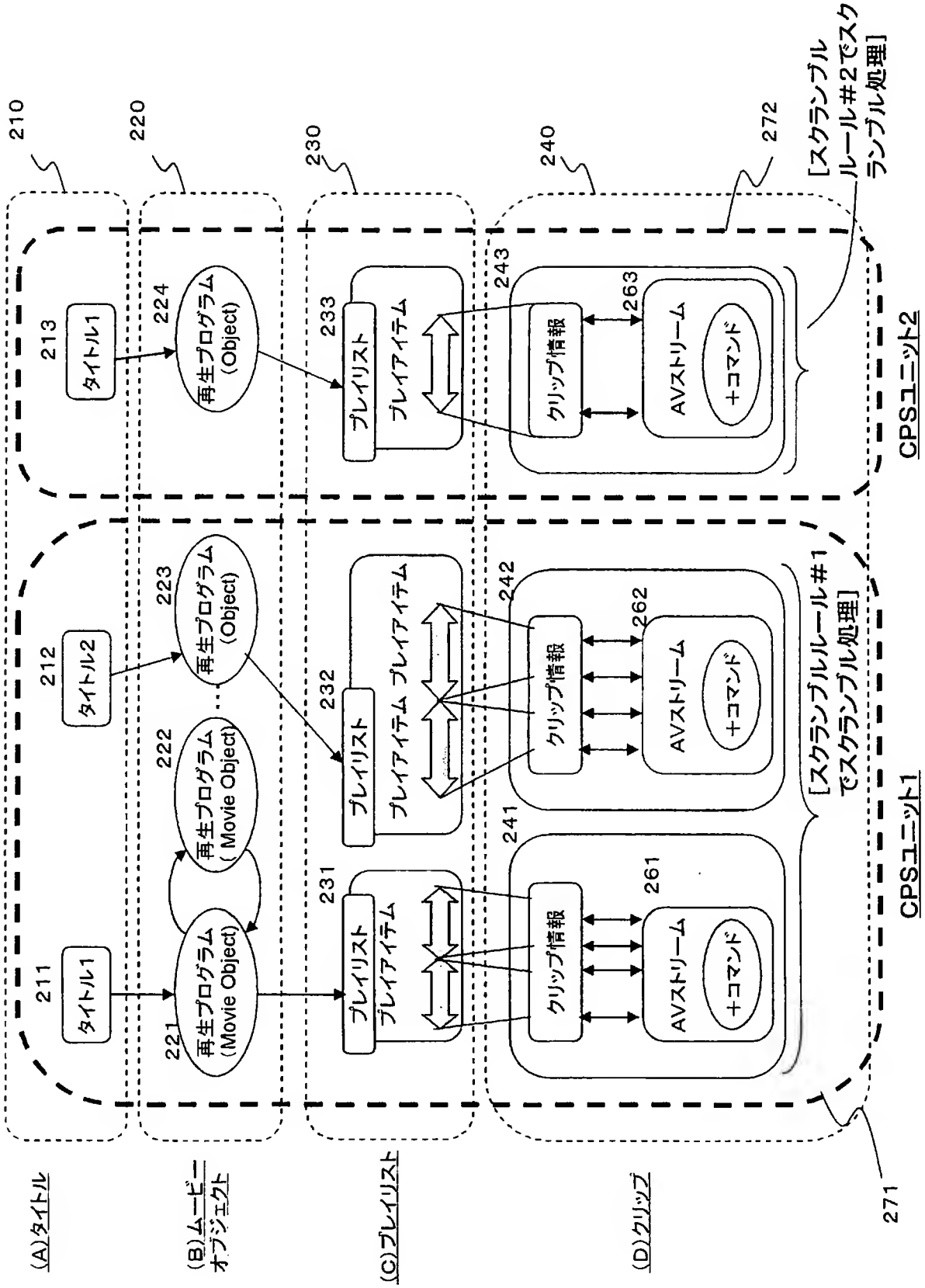
前記スクランブルルール解析ステップの解析結果、取得したコンテンツ固有のスクランブルルールに対応するスクランブル解除処理を実行するスクランブル解除ステップと、

を有することを特徴とするコンピュータ・プログラム。

[図1]


150
情報処理装置(再生装置)
154
スクランブル解除実行部
153
デコード処理部
151
再生処理実行LSI
152
復号処理部
155
メモリ(デバイス鍵)
120
ドライブ
100
111
暗号化コンテンツ(Encrypted Content)(AVストリーム)
112
MKB
113
ボリュームID
114
使用許諾情報
115
タイトル鍵データ
116
スクランブルルール

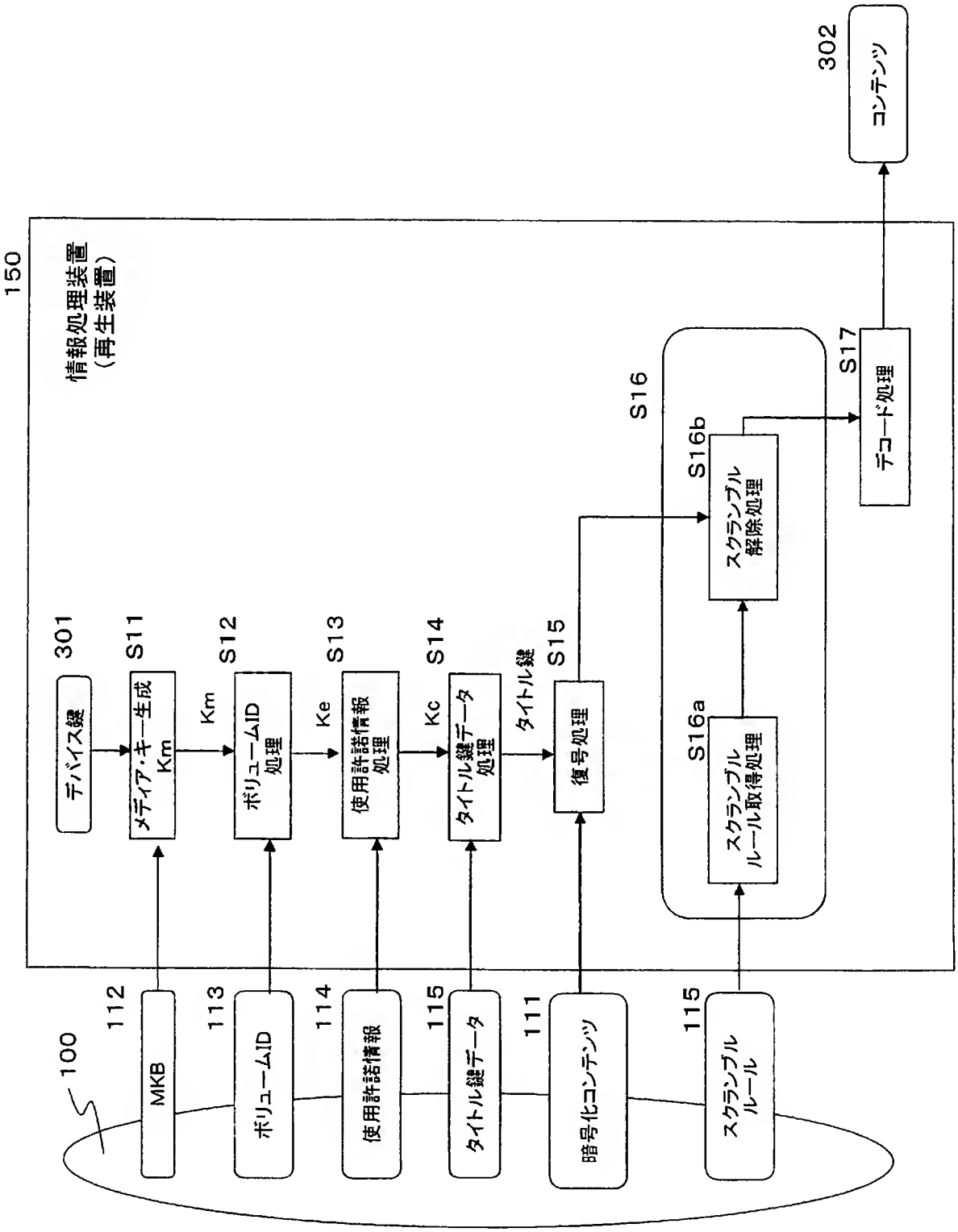
[図2]


(A)タイトル
(B)ムービーオブジェクト
(C)プレイリスト
(D)クリップ
210
220
230
240
271
272
211
タイトル1
212
タイトル2
213
タイトル1
221
再生プログラム (Movie Object)
222
再生プログラム (Movie Object)
223
再生プログラム (Object)
224
再生プログラム (Object)
231
プレイリスト
プレイアイテム
232
プレイリスト
プレイアイテム
プレイアイテム
233
プレイリスト
プレイアイテム
241
クリップ情報
AVストリーム
+コマンド
261
242
クリップ情報
AVストリーム
+コマンド
262
243
クリップ情報
AVストリーム
+コマンド
263
[スクランブルルール#1でスクランブル処理]
[スクランブルルール#2でスクランブル処理]
CPSユニット1
CPSユニット2

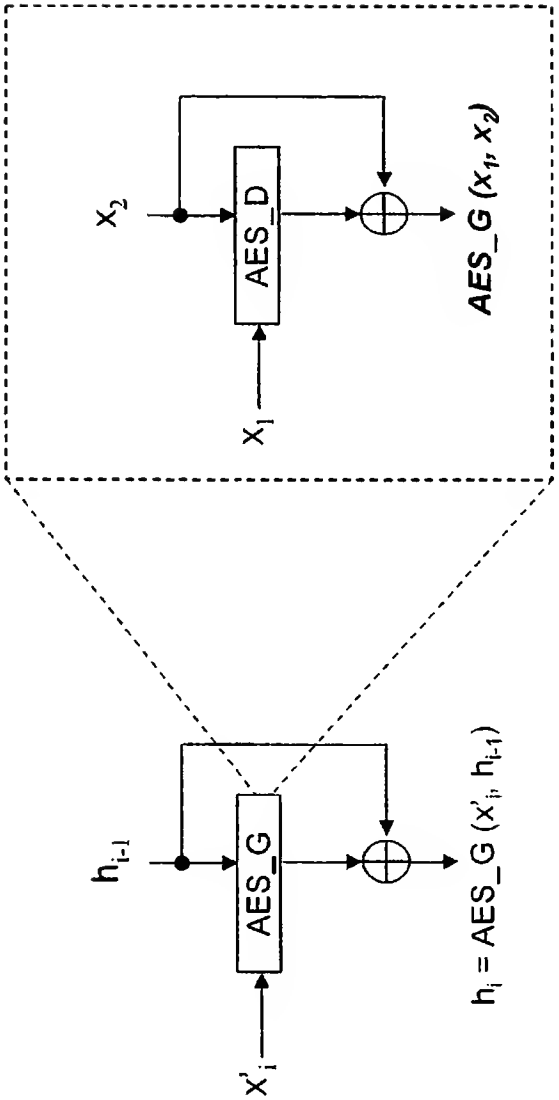
[図3]

タイトル等、アプリケーション層において区別可能なインデックス	コンテンツ管理ユニット(CPS)	スクランブルルール
タイトル1	CPS1	Scr#1
タイトル2	CPS1	Scr#1
アプリケーション1	CPS2	Scr#2
アプリケーション2	CPS3	Scr#3
：	：	：
データグループ1	CPS4	Scr#4
データグループ2	CPS5	Scr#5
：	：	：

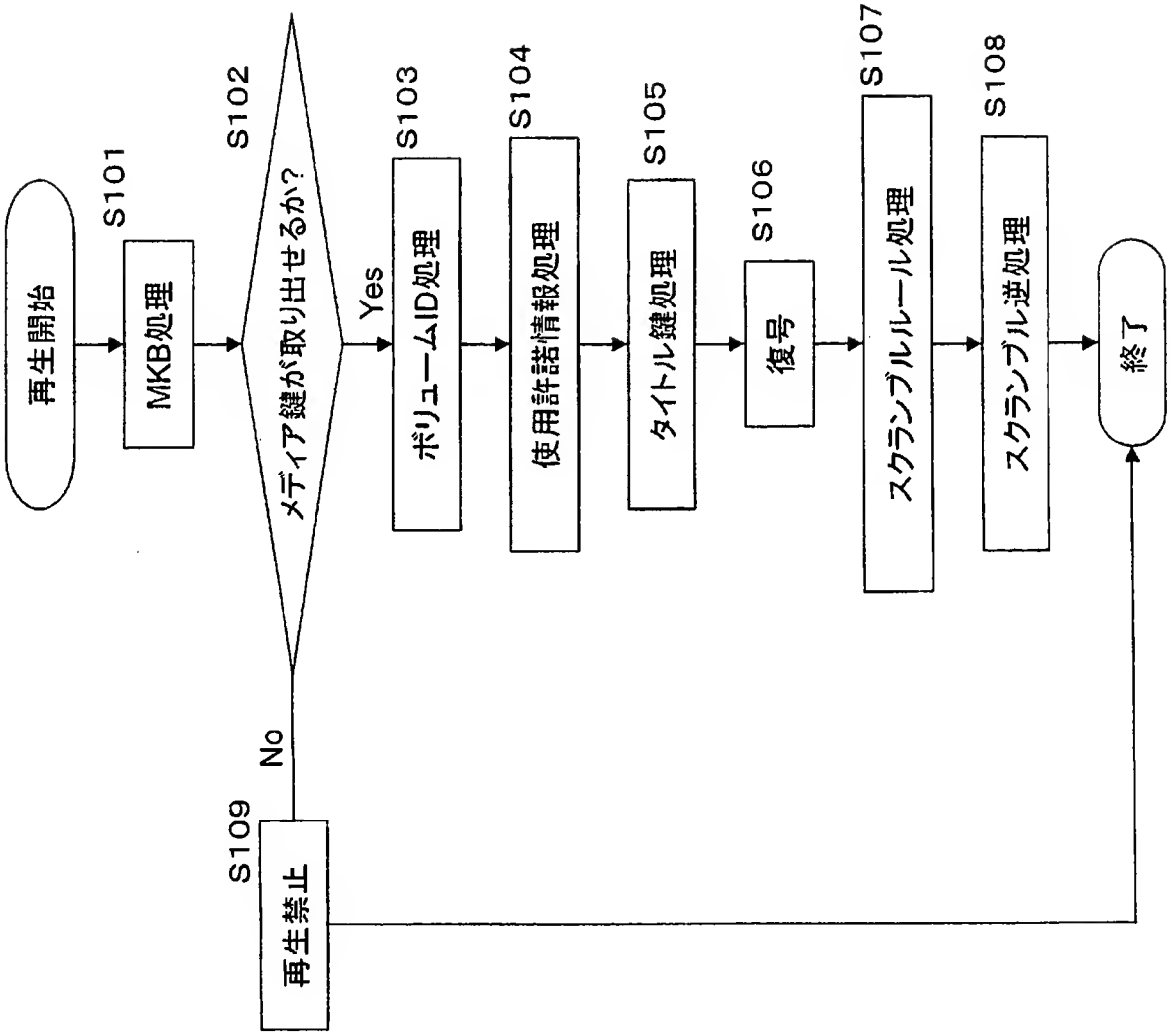
[図4]


100
MKB
112
ボリュームID
113
使用許諾情報
114
タイトル鍵データ
115
暗号化コンテンツ
111
スクランブル
ルール
115
150
情報処理装置
(再生装置)
301
デバイス鍵
S11
メディア・キー生成
Km
Km
S12
ボリュームID
処理
Ke
S13
使用許諾情報
処理
Kc
S14
タイトル鍵データ
処理
タイトル鍵
S15
復号処理
S16
S16a
スクランブル
ルール取得処理
S16b
スクランブル
解除処理
S17
デコード処理
302
コンテンツ

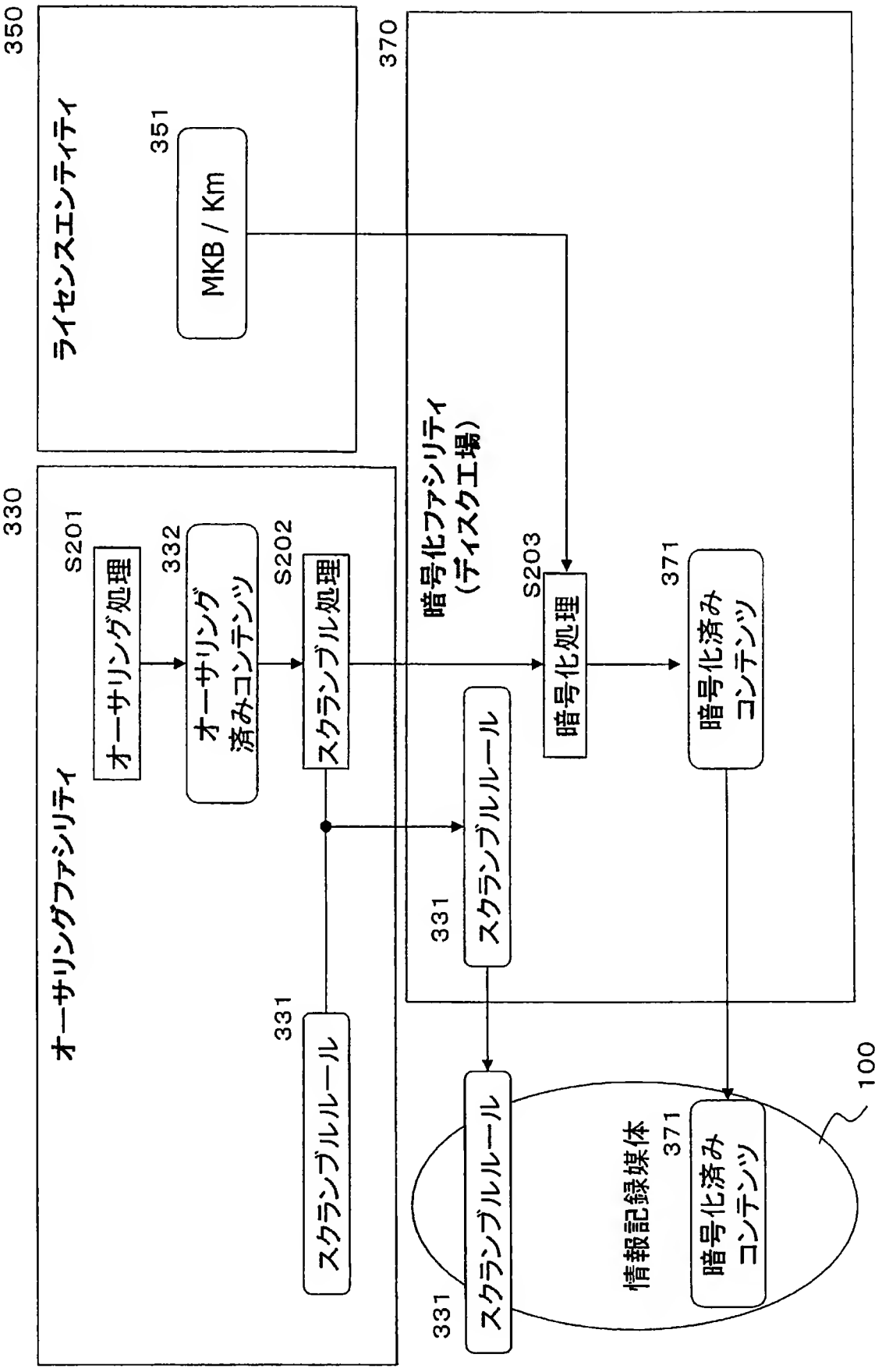
[図5]



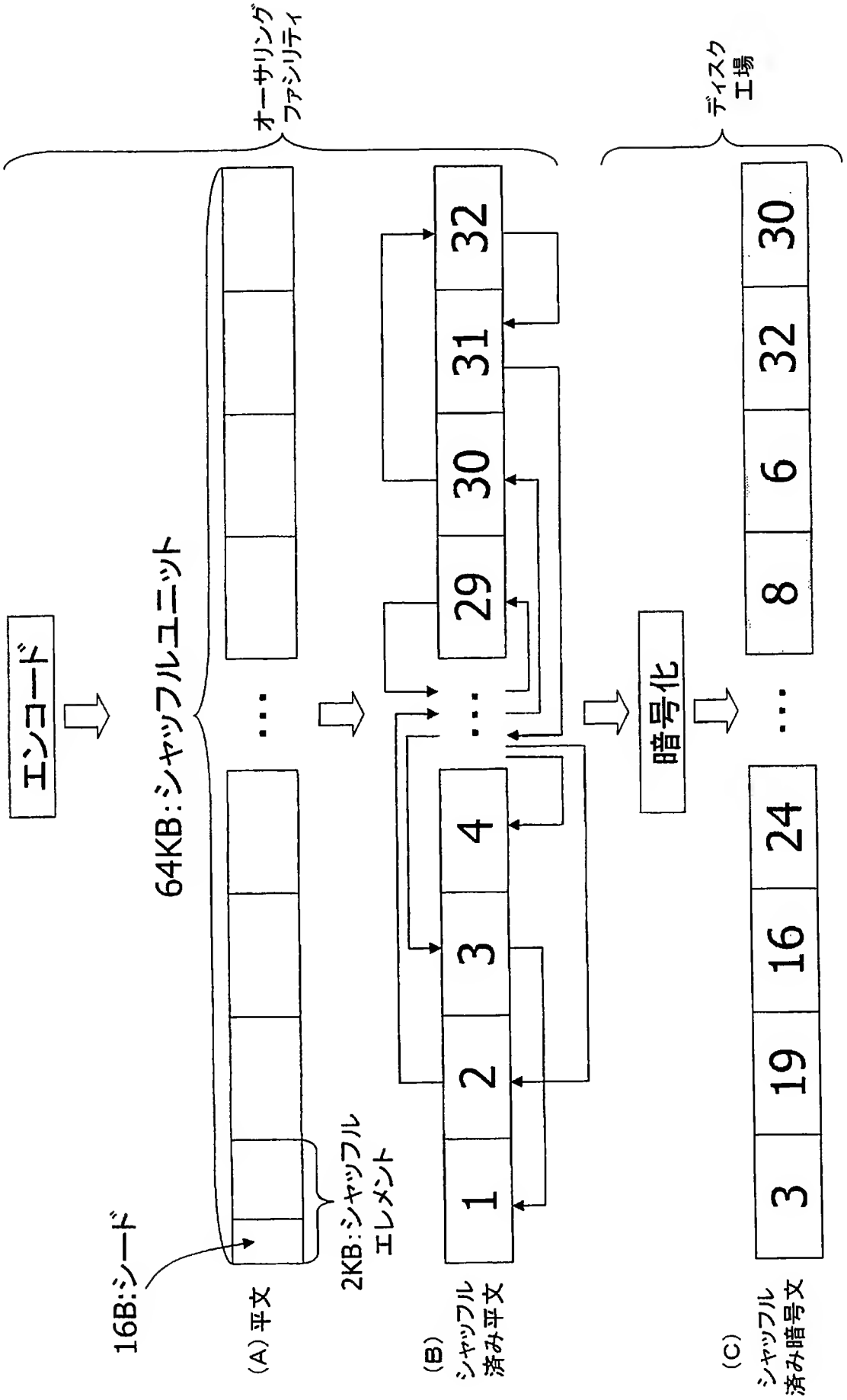
[図6]


再生開始
S101
MKB処理
S102
メディア鍵が取り出せるか?
Yes
No
S103
ボリュームID処理
S104
使用許諾情報処理
S105
タイトル鍵処理
S106
復号
S107
スクランブルルール処理
S108
スクランブル逆処理
S109
再生禁止
終了

[図7]


350
ライセンスエンティティ
351
MKB / Km
370
暗号化ファシリティ
(ディスク工場)
330
オーサリングファシリティ
S201
オーサリング処理
332
オーサリング
済みコンテンツ
S202
スクランブル処理
S203
暗号化処理
371
暗号化済み
コンテンツ
331
スクランブルルール
331
スクランブルルール
情報記録媒体
371
暗号化済み
コンテンツ
100

[図8]


オーサリング
ファシリティ
ディスク
工場
エンコード
64KB:シャッフルユニット
暗号化
16B:シード
2KB:シャッフル
エレメント
(A) 平文
(B)
シャッフル
済み平文
(C)
シャッフル
済み暗号文
1
2
3
4
29
30
31
32
3
19
16
24
8
6
32
30

[図9]

(A)スクランブルルール(シャッフルユニット内のシャッフルエレメントが32個の場合)

3	19	16	24	26	18	10	2
28	20	12	4	1	15	25	9
22	11	21	31	7	29	13	23
5	17	27	14	8	6	32	30

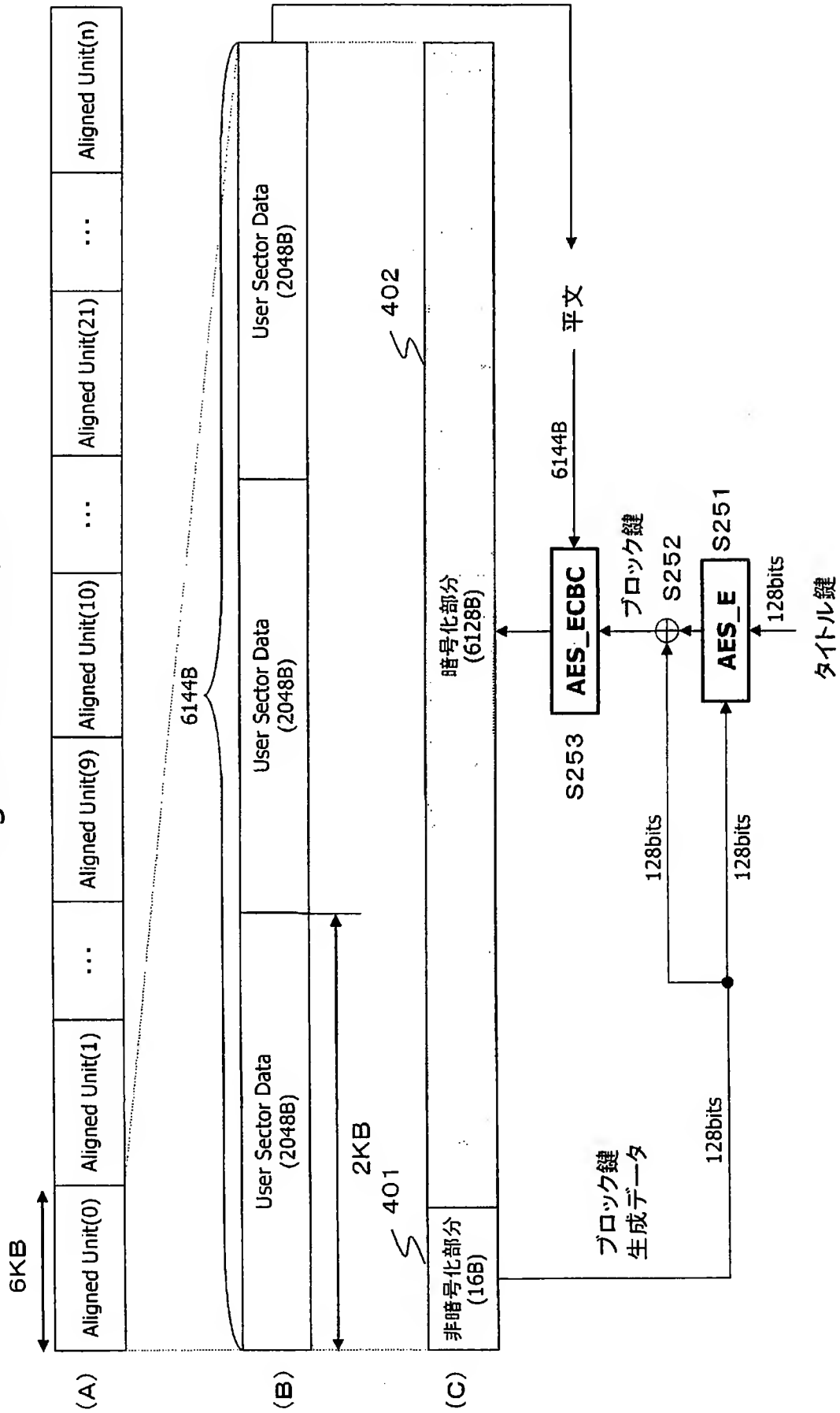
(B1)シャッフル前

												.....					
1	2	3	4	5	6	7	8	9	10	11	12	.....	28	29	30	31	32

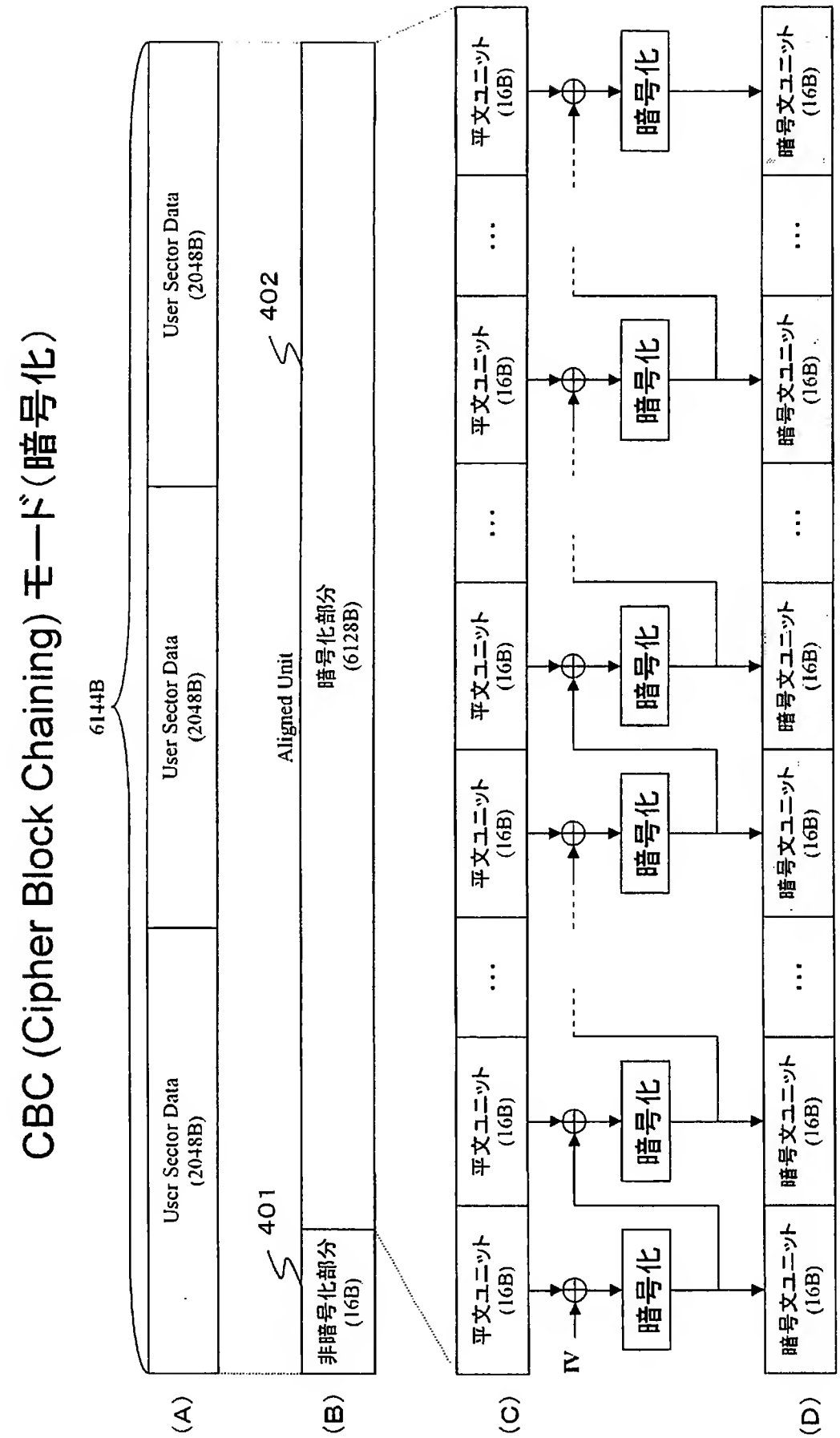
(B2)シャッフル後

												.....					
3	19	16	24	26	18	10	2	28	20	12	4	.....	14	8	6	32	30

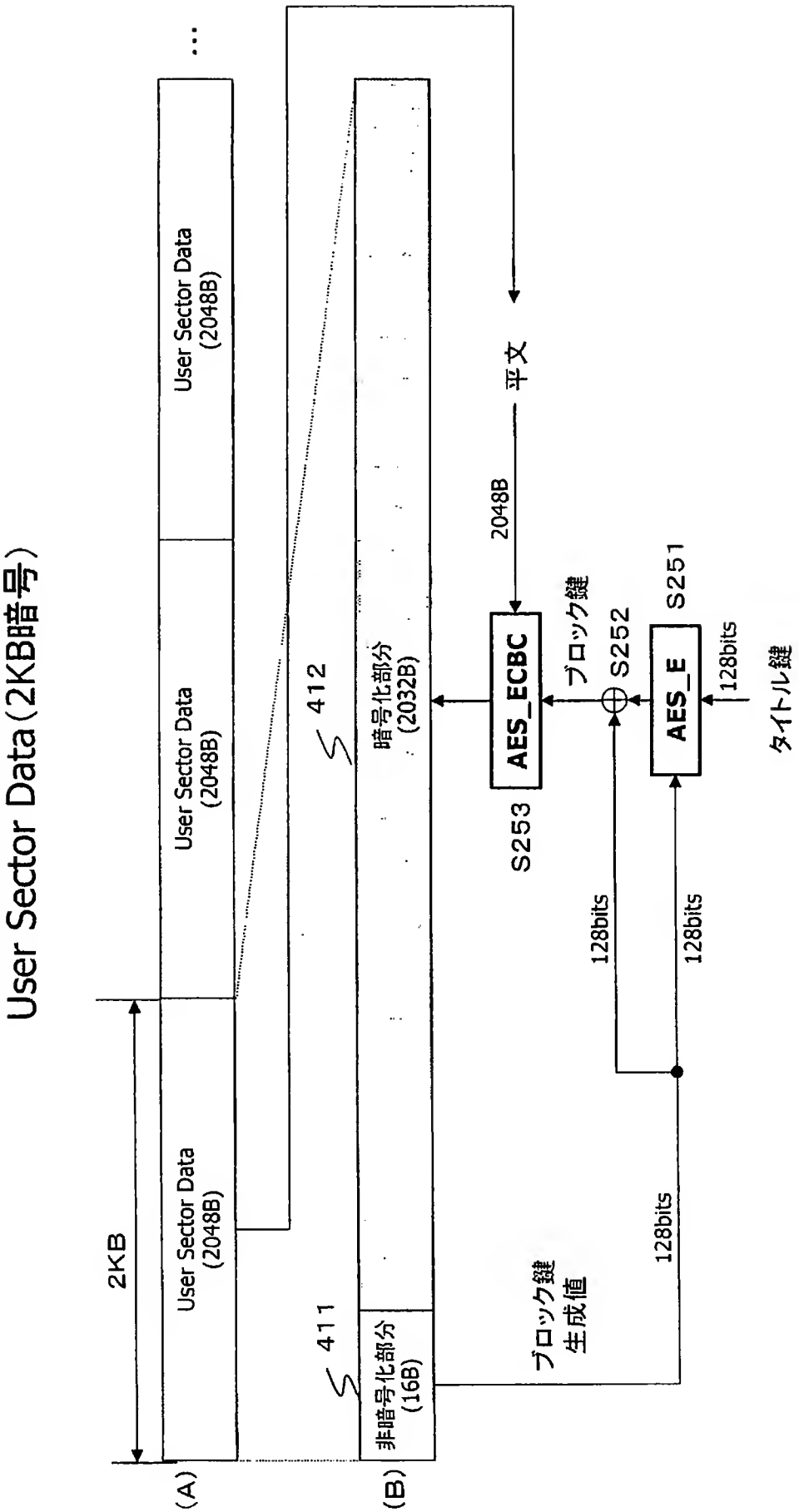
[図10]


Aligned Unit(6KB暗号)
6KB
Aligned Unit(0)
Aligned Unit(1)
...
Aligned Unit(9)
Aligned Unit(10)
...
Aligned Unit(21)
...
Aligned Unit(n)
(A)
(B)
(C)
6144B
User Sector Data (2048B)
User Sector Data (2048B)
User Sector Data (2048B)
2KB
401
402
非暗号化部分 (16B)
暗号化部分 (6128B)
6144B
平文
S253
AES_ECBC
ブロック鍵
S252
AES_E
S251
128bits
タイトル鍵
128bits
128bits
128bits
ブロック鍵
生成データ

[図11]


CBC (Cipher Block Chaining) モード(暗号化)
6144B
User Sector Data (2048B)
User Sector Data (2048B)
User Sector Data (2048B)
Aligned Unit
402
401
非暗号化部分 (16B)
暗号化部分 (6128B)
平文ユニット (16B)
暗号化
暗号文ユニット (16B)
IV
(A)
(B)
(C)
(D)

[図12]


User Sector Data(2KB暗号)
User Sector Data (2048B)
User Sector Data (2048B)
User Sector Data (2048B)
...
2KB
(A)
(B)
非暗号化部分 (16B)
暗号化部分 (2032B)
411
412
ブロック鍵 生成値
128bits
128bits
128bits
AES_ECBC
AES_E
S253
S252
S251
ブロック鍵
タイトル鍵
2048B
平文

[図13]

MSTBL.DAT(ディスク工場での暗号化用の補助ファイル)

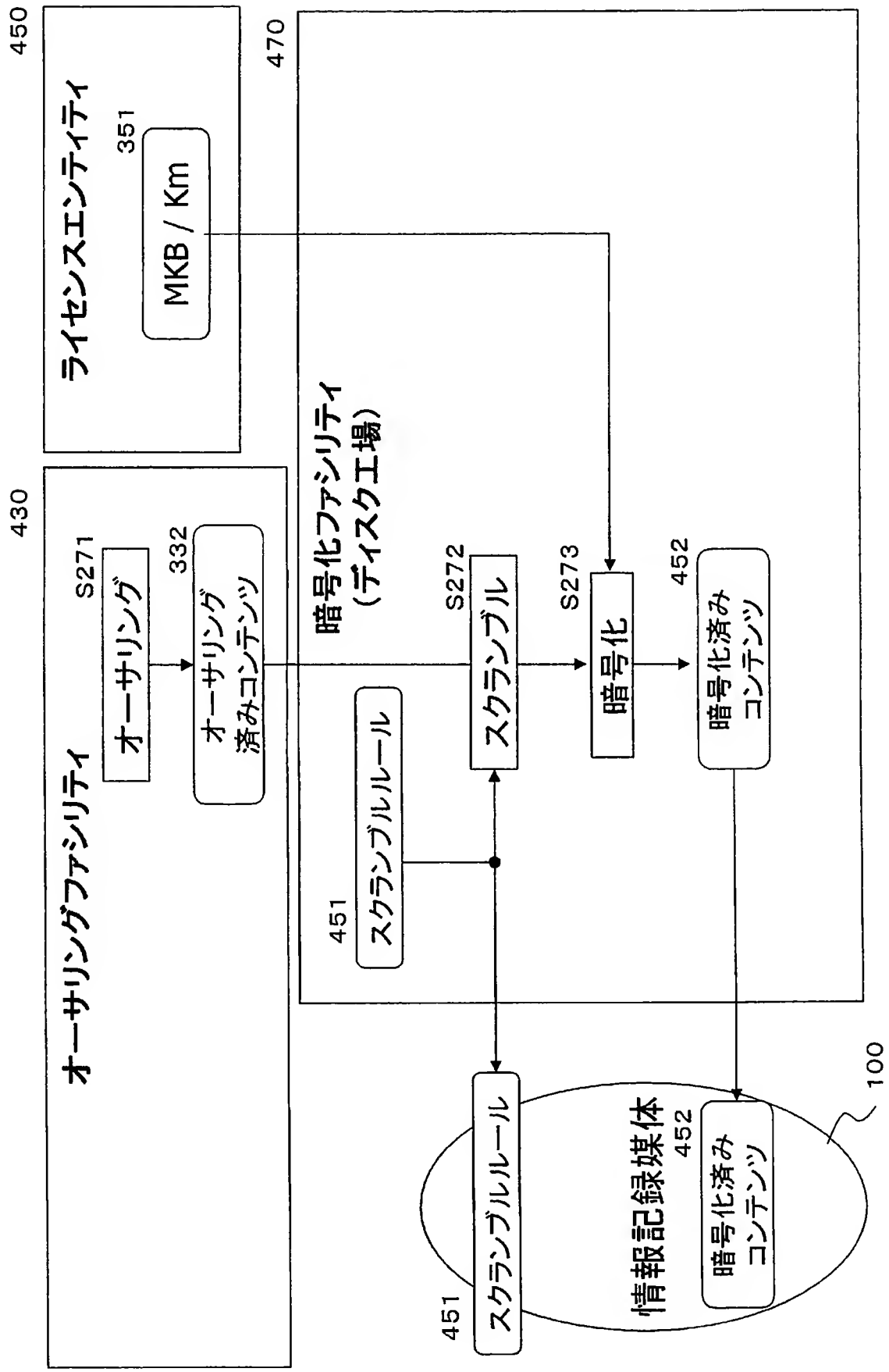
	#bits	value
Li_MSTBL.DAT( ){		
UD_START_Location	32	
UD_END_Location	32	
CHT_Location	32	
CHT_Offset	32	
Content_Cert_Location	32	
Content_Cert_Offset	32	
UK_Inf_Location	32	
UK_Inf_Offset	32	
Num_of_UK	32	
MKB_Location	32	
For (j = 1; j =<N, j++) {		
Encryption_Flag(j)	8	00_{16} : not to-be-encrypted 01_{16} : to-be-encrypted
Data_Type(j)	8	01_{16} : 1st sector of AU 02_{16} : 2nd sector of AU 03_{16} : 3rd sector of AU 04_{16} : Non-AV data (e.g. Java)
CPS_Unit_No(j)	16	0000_{16}-$FFFF_{16}$
Clip_AV_File_No(j)	24	00000-99999
Reserved	6	000000_2
Last_Sector_of_Clip(j)	1	0_2 : not Last Sector of each Clip 1_2 : Last Sector of each Clip
Last_Sector_of_Layer(j)	1	0_2 : not Last Sector of each Clip in layer i 1_2 : Last Sector of each Clip in each layer i
}		
}		

[図14]

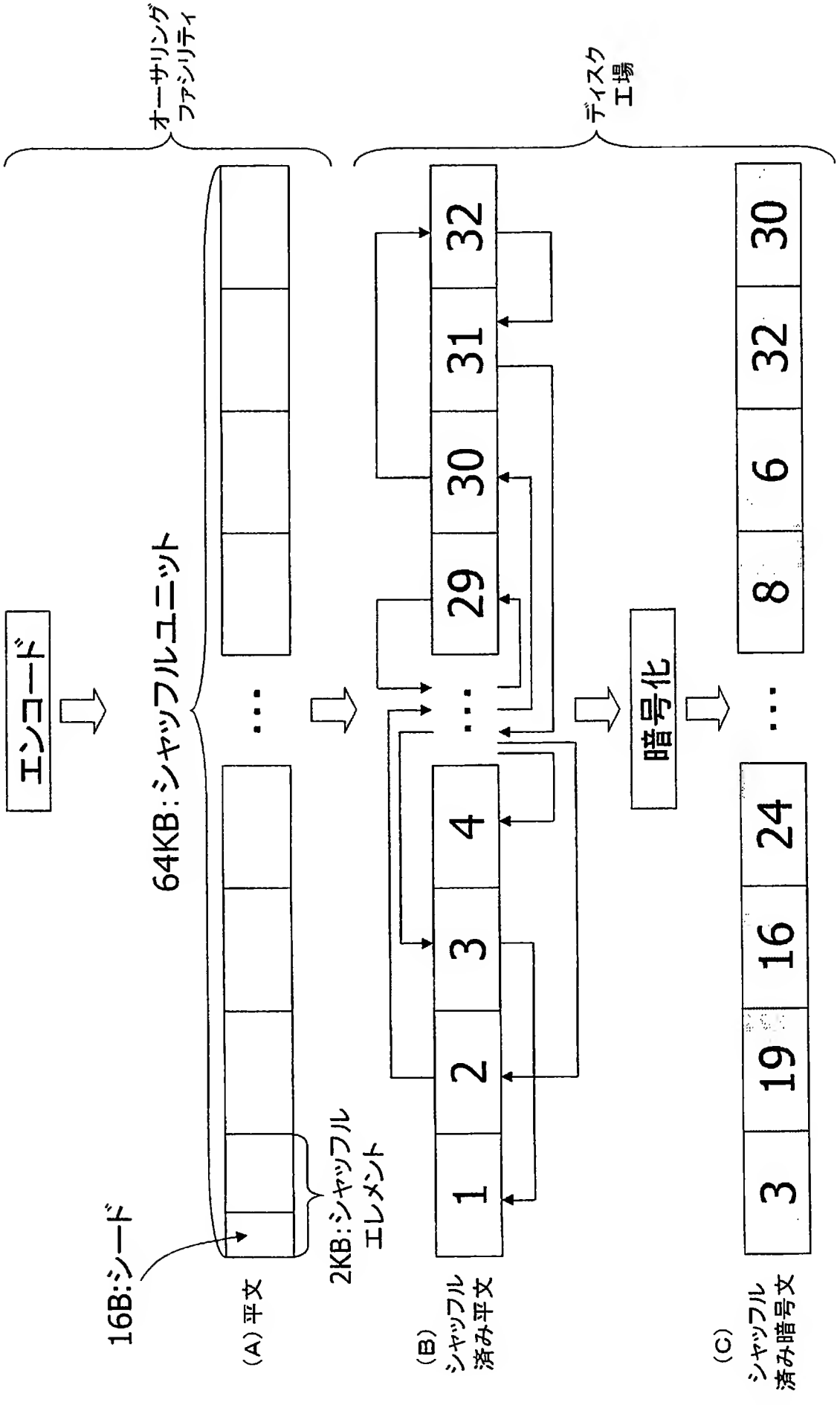
MSTBL.DATのシンタックス

UD_START_Location：各LayerのUser Data (Data Zone)の開始点のPhysical Sector Number。
UD_END_Location：各LayerのUser Data (Data Zone)の終了点のPhysical Sector Number。
CHT_Location：CHTの開始点のPhysical Sector Number。
CHT_Offset：CHTの開始点とHash Value(Mastering Facilityが埋めるデータ)の直前までのバイト数。
Content_Cert_Location：Content Certificateの開始点のPhysical Sector Number。
Content_Cert_Offset：Content Certificateの開始点とContent ID (Mastering Facilityが埋めるデータ)の直前までのバイト数。
UK_Inf_Location：タイトル鍵ファイルの開始点のPhysical Sector Number。そのLayerにUnit_Key.infが記録されない場合は、00000000_{16}を記述。
UK_Inf_Offset：Unit_Key.infの開始点とEncrypted Unit Key for CPS Unit#1の直前までのバイト数。そのLayerにUnit_Key.infが記録されない場合は、00000000_{16}を記述。
Num_of_UK：Disc全体のUnit Keyの数(＝CPS Unitの数)。
MKB_Location：MKBの開始点のPhysical Sector Number。そのLayerにMKB_Certが記録されない場合は、00000000_{16}を記述。
N：Layer i のLogical Sector数。
Encryption_Flag：暗号化するかしないかのFlag。
Data_Type：SectorのTypeを示すFlag。
CPS_Unit_No：CPS Unit Number。
Clip_AV_File_No：クリップファイル番号。CHT作成のために使う情報。
Last_Sector_of_Clip：(Layerに関わらず)各クリップの最終Sectorを示すフラグ。
Last_Sector_of_Layer：各Layerでの各クリップの最終Sectorを示すフラグ。

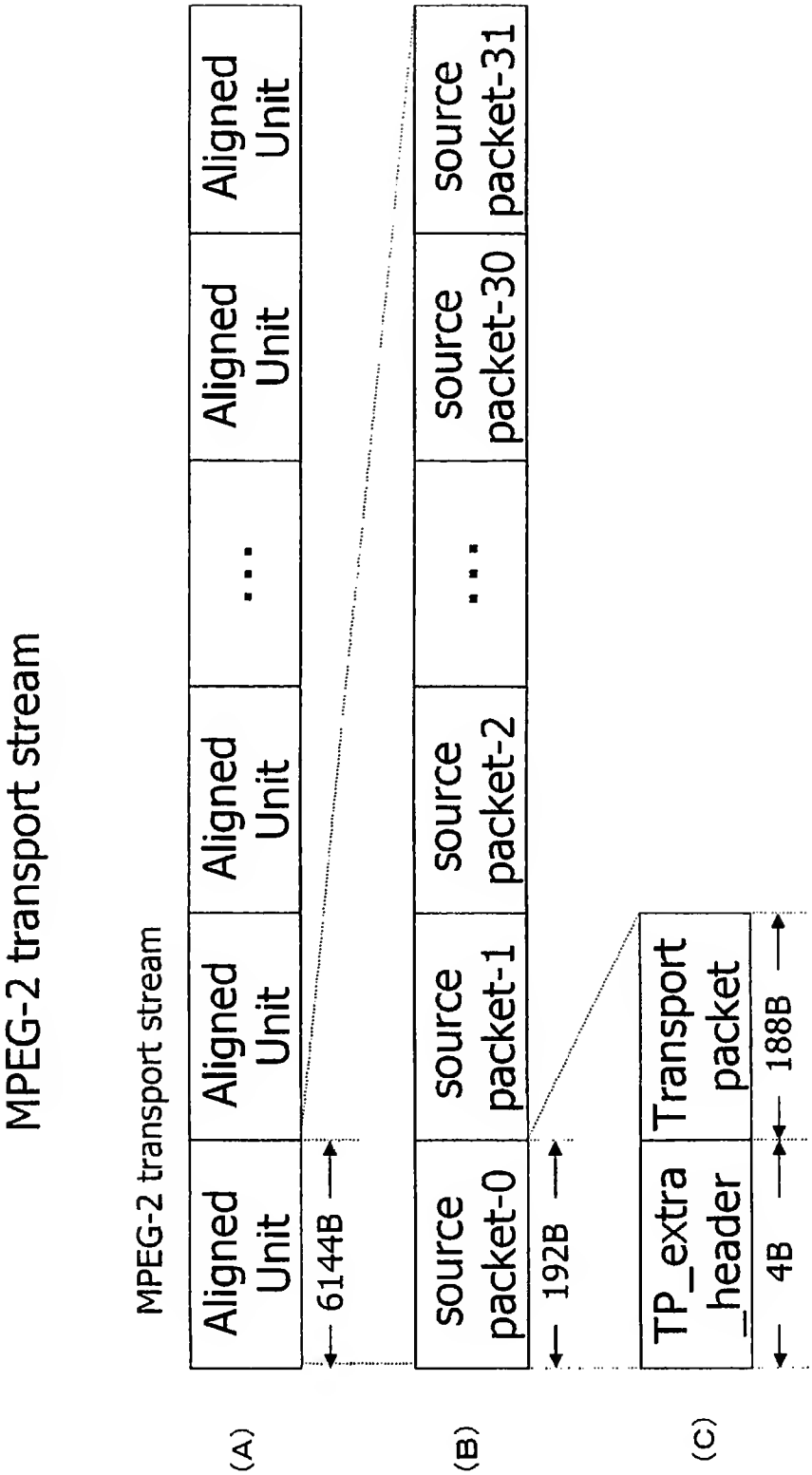
[図15]


450
ライセンスエンティティ
351
MKB / Km
470
暗号化ファシリティ
(ディスクエ場)
430
オーサリングファシリティ
S271
オーサリング
332
オーサリング
済みコンテンツ
451
スクランブルルール
S272
スクランブル
S273
暗号化
452
暗号化済み
コンテンツ
100
情報記録媒体
451
スクランブルルール
452
暗号化済み
コンテンツ

[図16]


オーサリング
ファシリティ
ディスク
工場
エンコード
64KB:シャッフルユニット
暗号化
16B:シード
2KB:シャッフル
エレメント
(A) 平文
(B)
シャッフル
済み平文
(C)
シャッフル
済み暗号文
1
2
3
4
29
30
31
32
3
19
16
24
8
6
32
30

[図17]


MPEG-2 transport stream
MPEG-2 transport stream
Aligned Unit
Aligned Unit
Aligned Unit
...
Aligned Unit
Aligned Unit
6144B
(A)
source packet-0
source packet-1
source packet-2
...
source packet-30
source packet-31
192B
(B)
TP_extra _header
Transport packet
4B
188B
(C)

[図18]

（A）source_packetのシンタックス

	#bits
source_packet(){	
TP_extra_header()	4
transport_packet()	188
}	

（B）TP_extra_headerのシンタックス

	#bits
TP_extra_header(){	
is_not_free	1
is_encrypted	1
arrival_time_stamp	30
}	

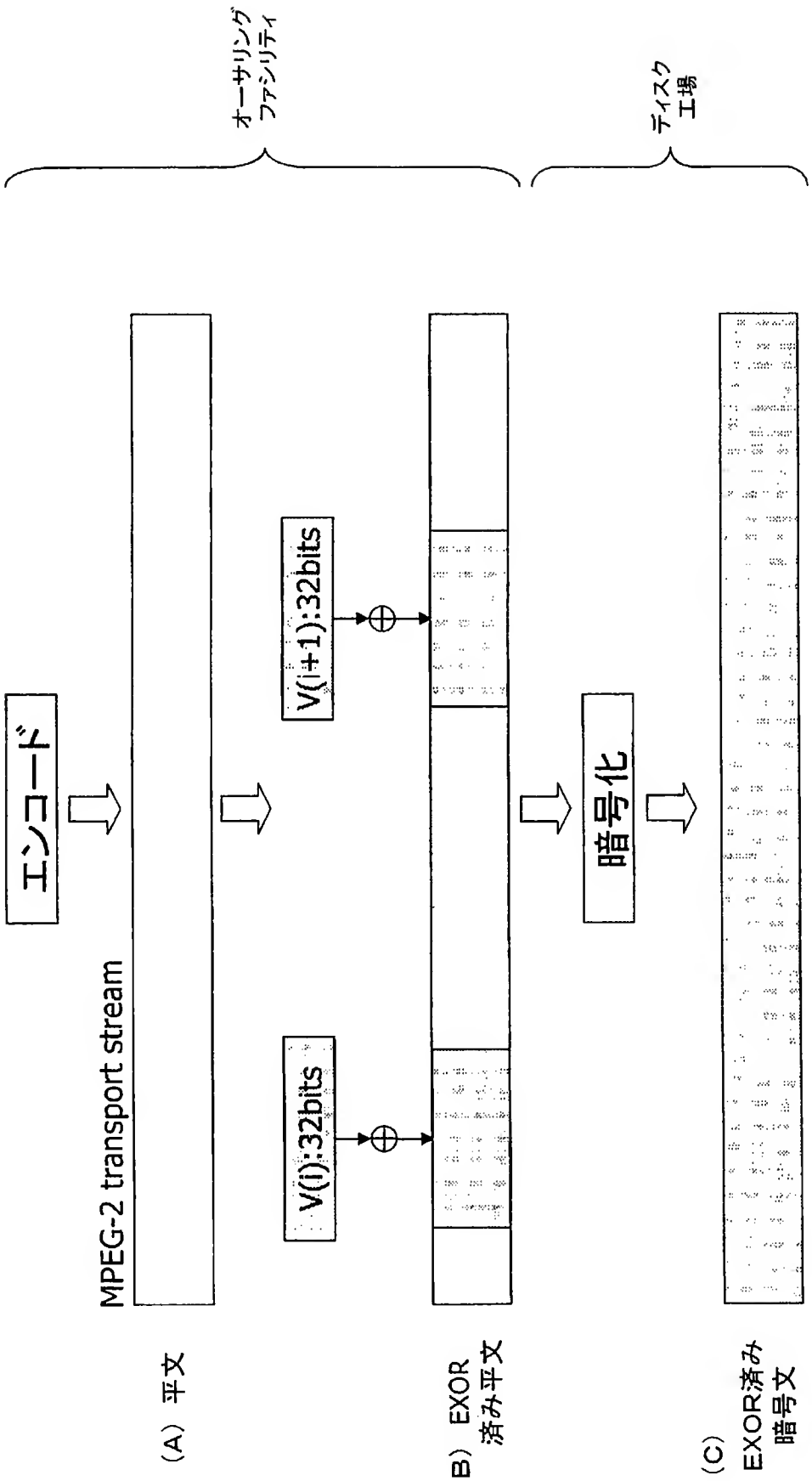
[図19]

transport_packetのシンタックス

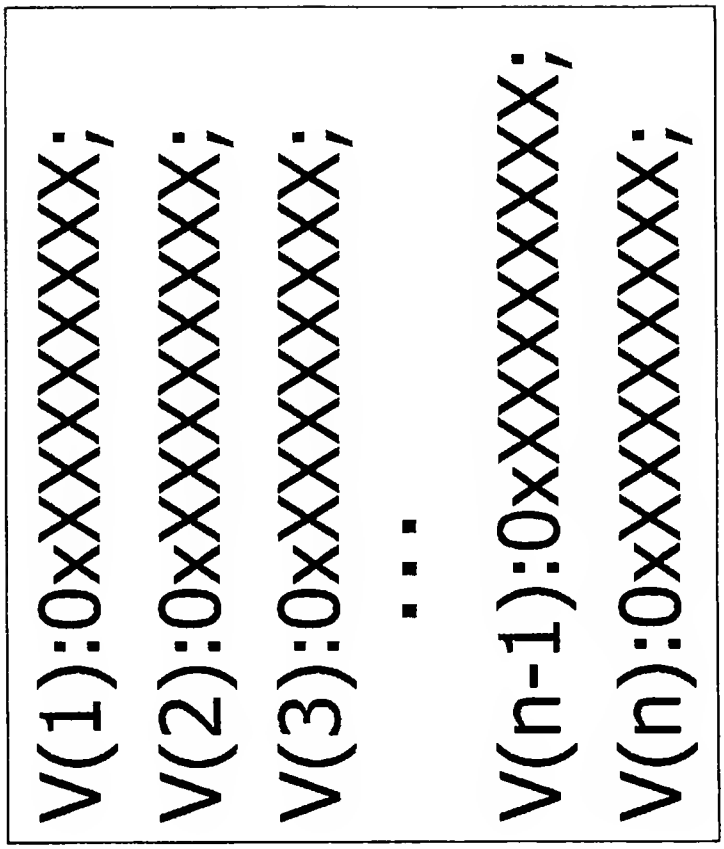
```
                                                    #bits
transport_packet(){
    sync_byte                                       8
    transport_error_indicator                       1
    payload_unit_start_indicator                    1
    transport_priority                              1
    PID                                             13
    transport_scrambling_contorl                    2
    adaptation_field_control                        2
    continuity_counter                              4
    if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {
        adaptation field()
    }
     if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {

        adaptation field()
    }
     if (adaptation_field_control==‘ || adaptation_filed_control==’11’) {
        for (i=0; i<N; i++) {
            data_byte                               8
        }
    }
}
```

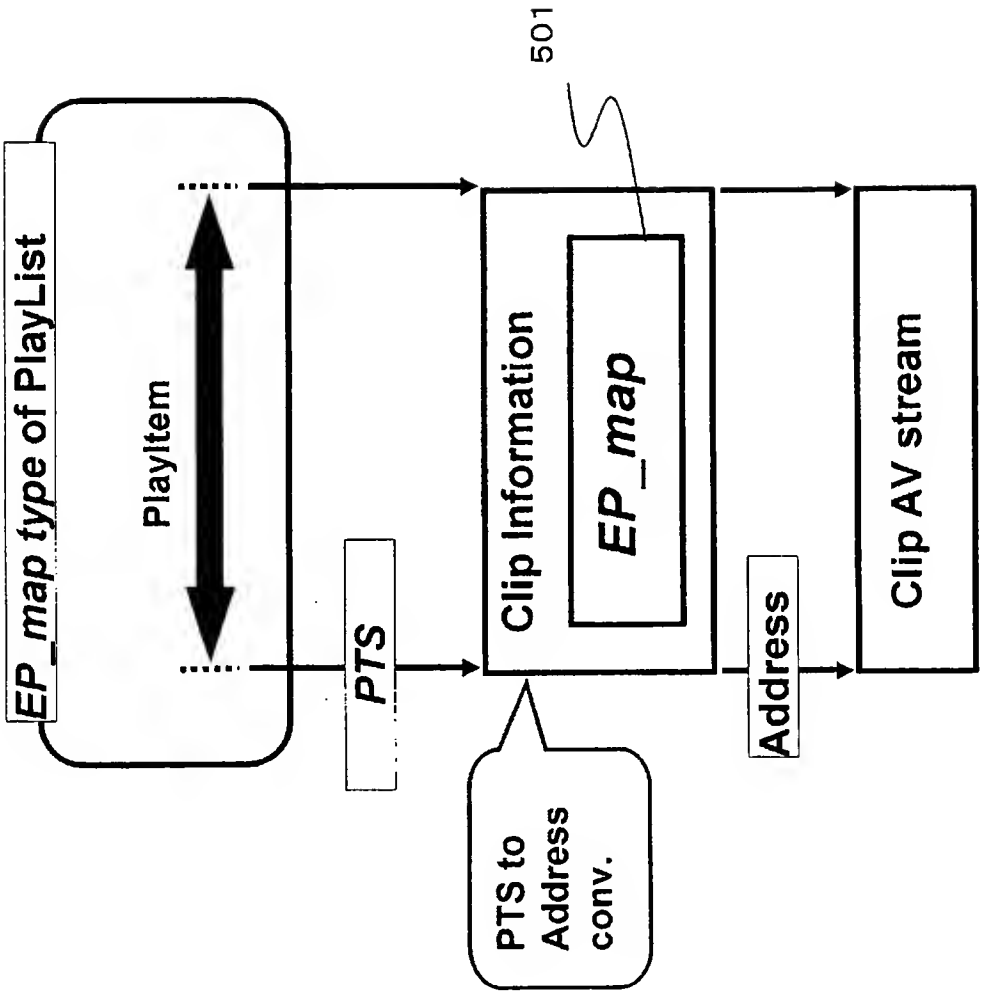
[図20]


オーサリング
ファシリティ
ディスク
工場
エンコード
MPEG-2 transport stream
V(i):32bits
V(i+1):32bits
暗号化
(A) 平文
(B) EXOR
済み平文
(C)
EXOR済み
暗号文

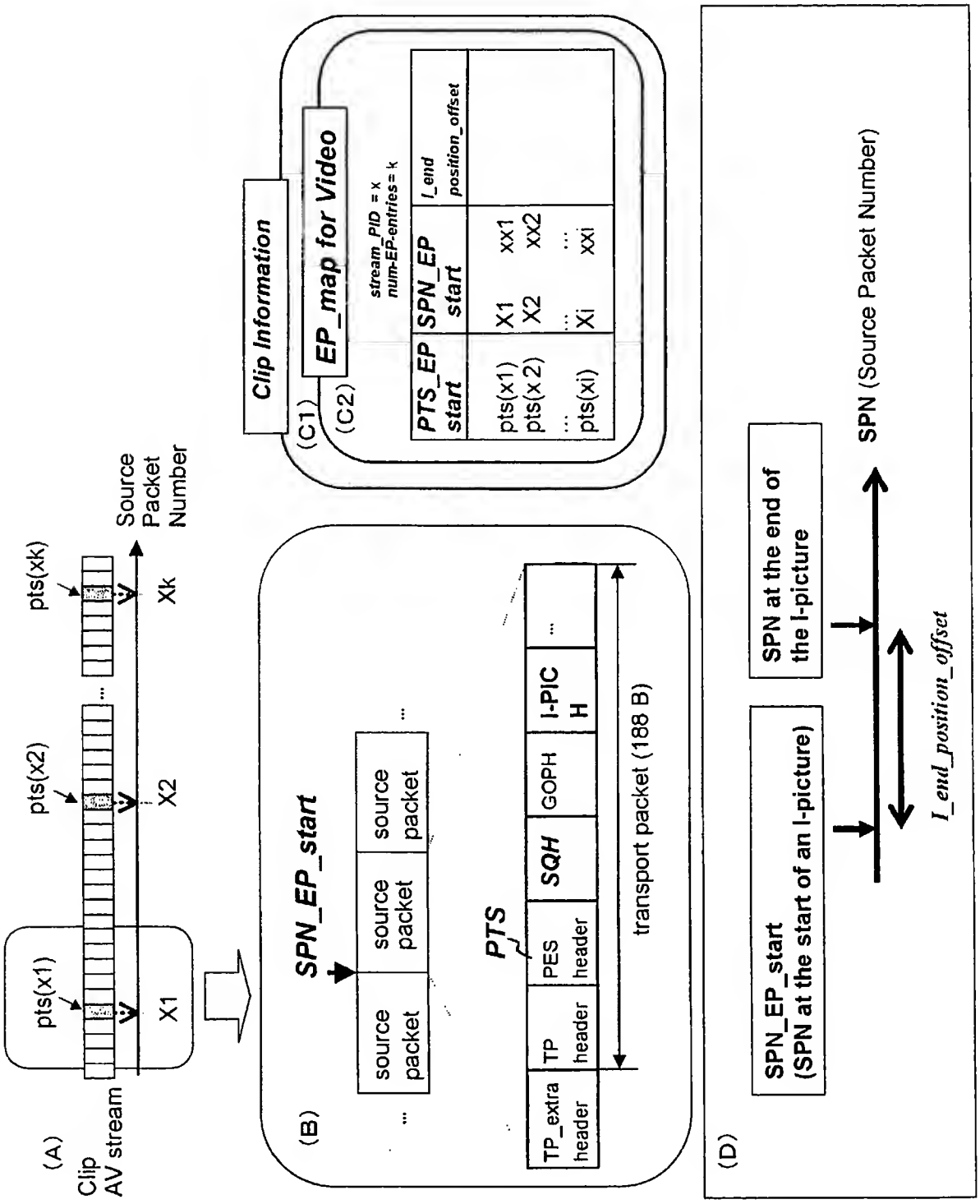
[図21]


V(1):0xXXXXXXXX;
V(2):0xXXXXXXXX;
V(3):0xXXXXXXXX;
...
V(n-1):0xXXXXXXXX;
V(n):0xXXXXXXXX;

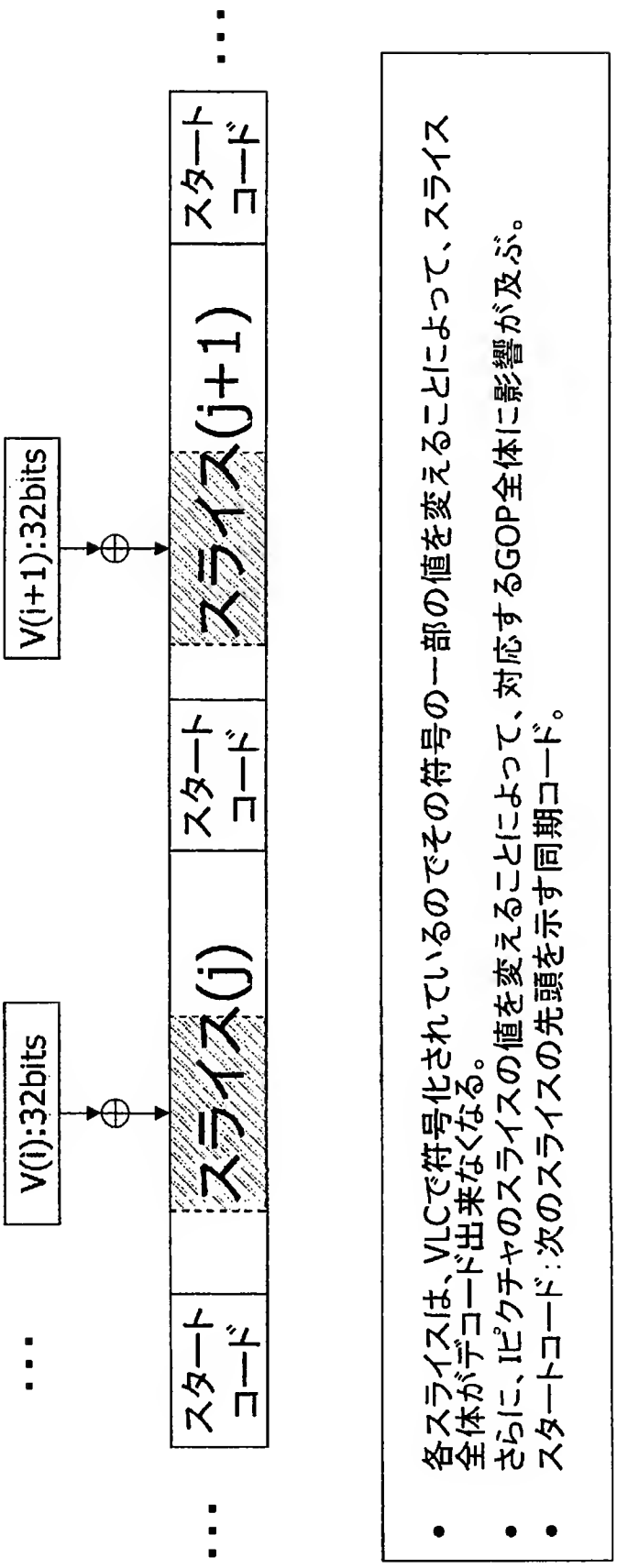
[図22]


501
EP_map type of PlayList
PlayItem
PTS
Clip Information
EP_map
Address
Clip AV stream
PTS to Address conv.

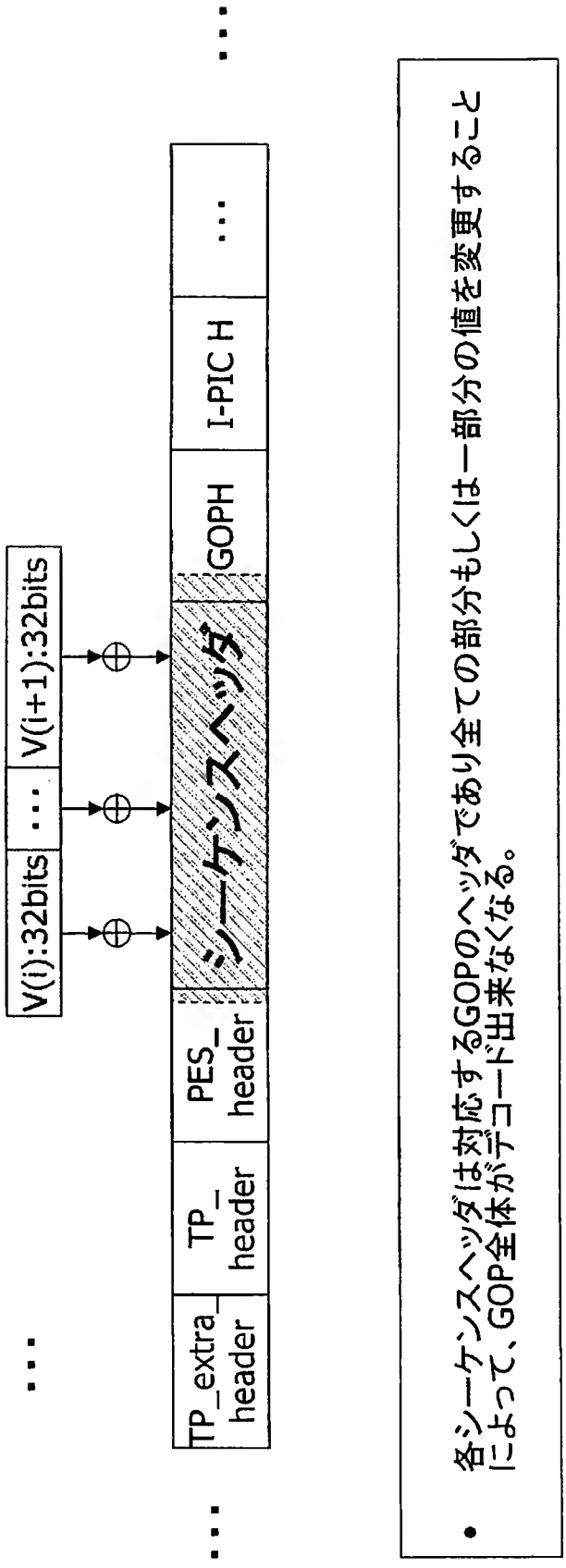
[図23]


(A)
Clip
AV stream
pts(x1)
pts(x2)
pts(xk)
X1
X2
Xk
Source
Packet
Number
(B)
SPN_EP_start
source packet
PTS
TP_extra header
TP header
PES header
SQH
GOPH
I-PIC H
transport packet (188 B)
Clip Information
(C1)
EP_map for Video
(C2)
stream_PID = x
num-EP-entries = k
PTS_EP start
SPN_EP start
I_end position_offset
pts(x1) X1 xX1
pts(x 2) X2 xX2
pts(xi) Xi xXi
(D)
SPN_EP_start
(SPN at the start of an I-picture)
SPN at the end of
the I-picture
SPN (Source Packet Number)
I_end_position_offset

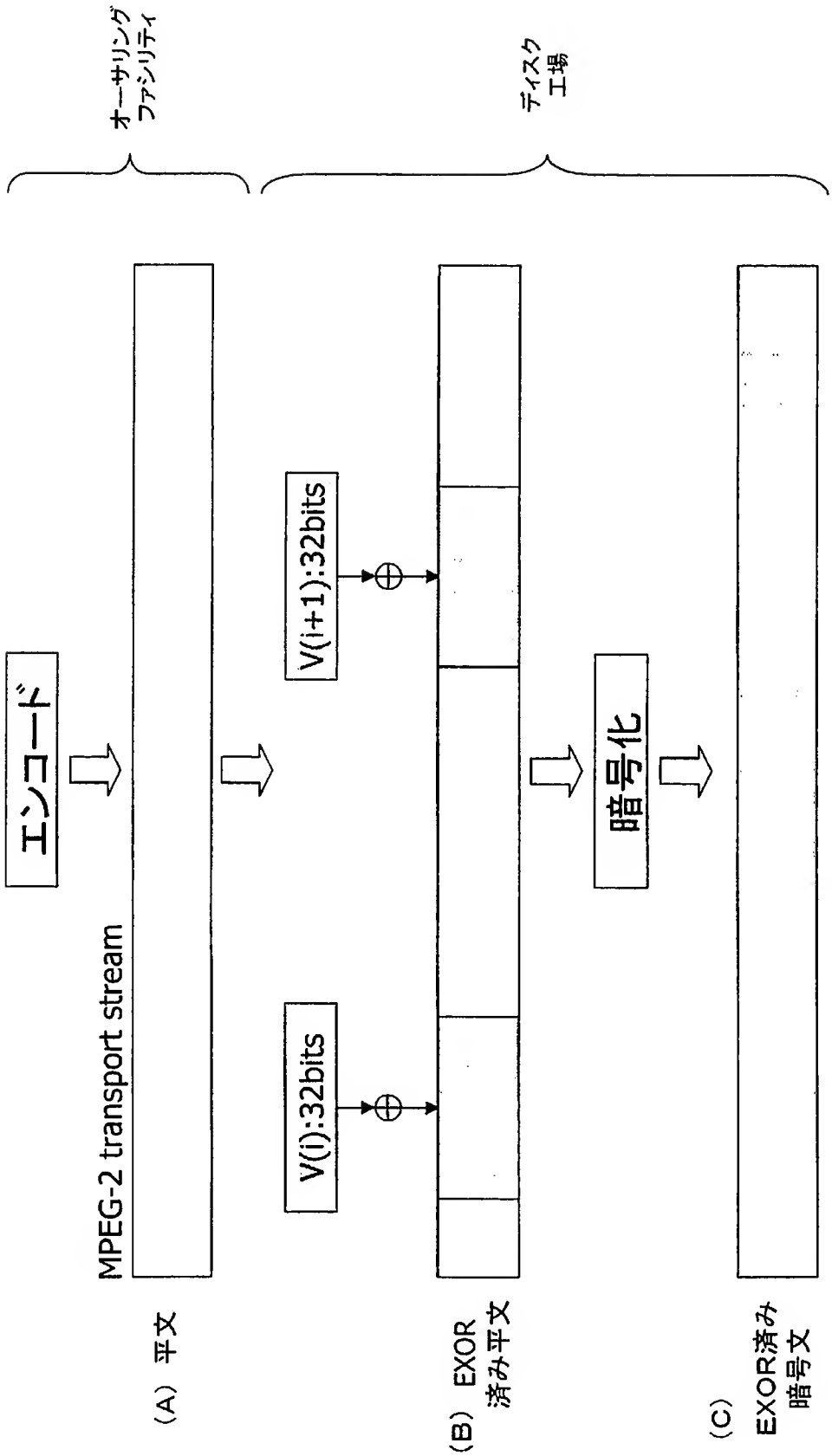
[図24]


V(i):32bits
V(i+1):32bits
スタートコード
スライス(j)
スタートコード
スライス(j+1)
スタートコード
・各スライスは、VLCで符号化されているのでその符号の一部の値を変えることによって、スライス全体がデコード出来なくなる。
・さらに、Iピクチャのスライスの値を変えることによって、対応するGOP全体に影響が及ぶ。
・スタートコード：次のスライスの先頭を示す同期コード。

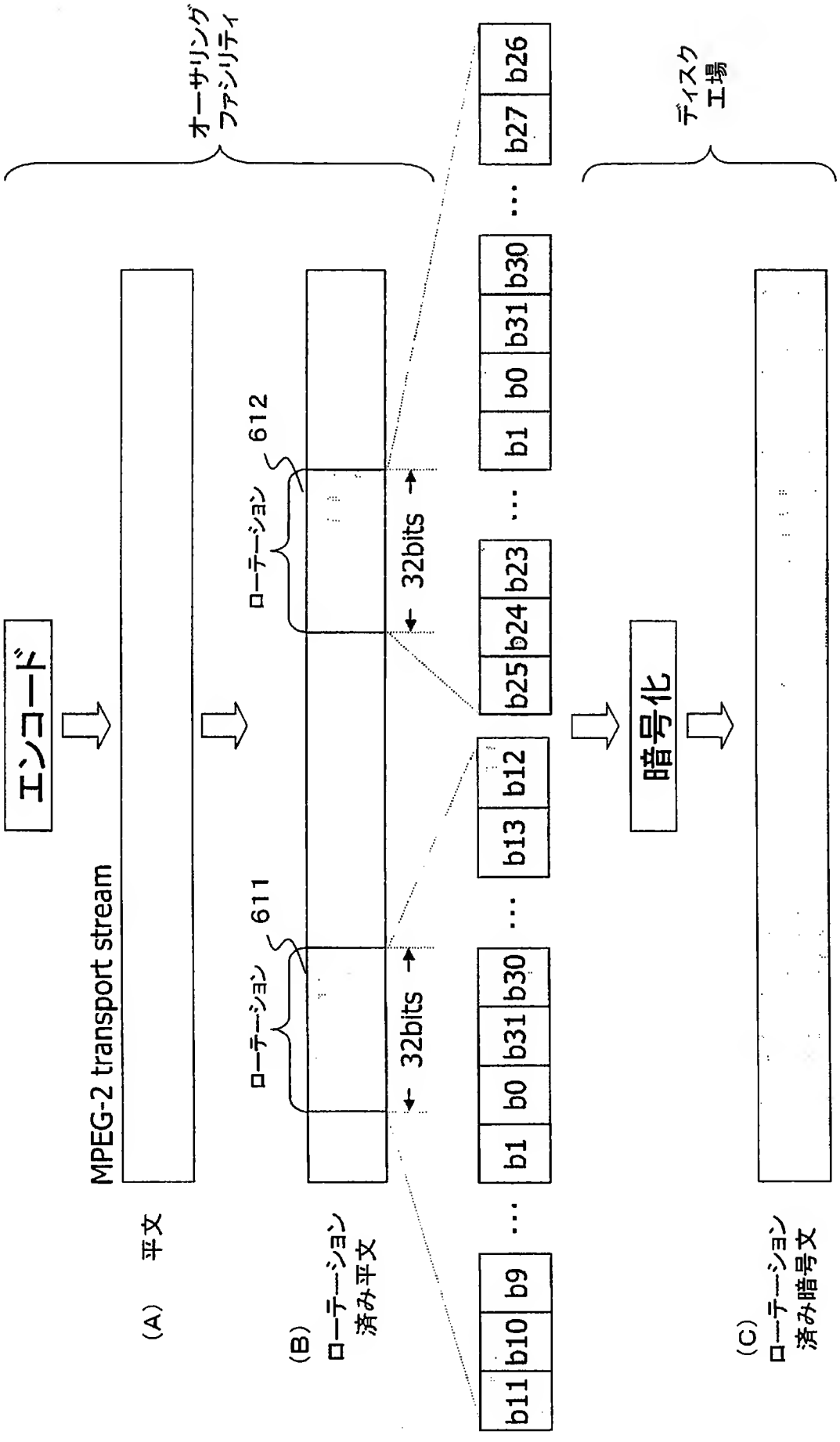
[図25]


V(i):32bits
V(i+1):32bits
TP_extra_header
TP_header
PES_header
シーケンスヘッダ
GOPH
I-PIC H
・各シーケンスヘッダは対応するGOPのヘッダであり全ての部分もしくは一部分の値を変更することによって、GOP全体がデコード出来なくなる。

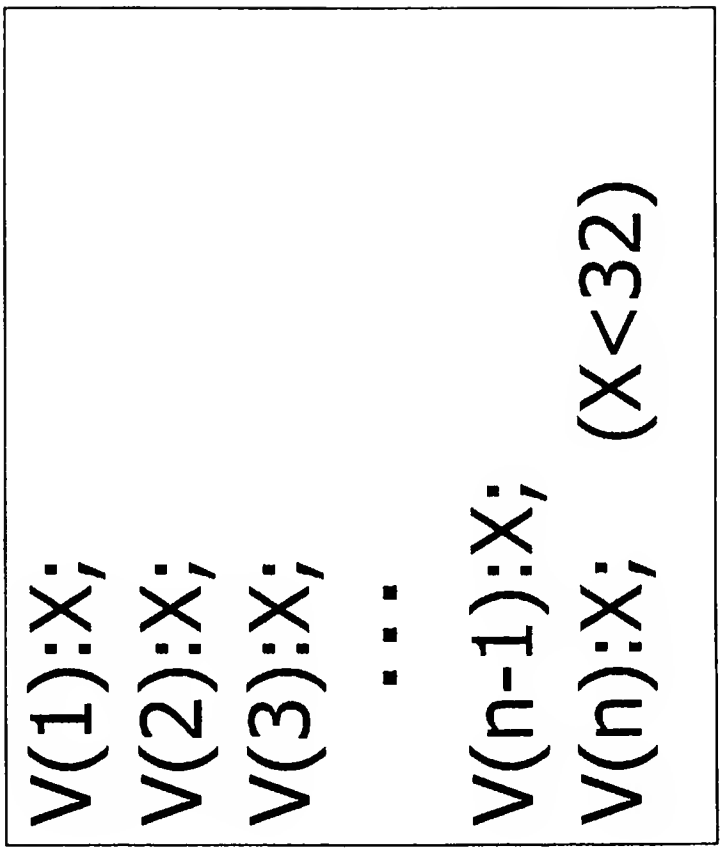
[図26]


オーサリング
ファシリティ
ディスク
工場
エンコード
MPEG-2 transport stream
V(i):32bits
V(i+1):32bits
暗号化
(A) 平文
(B) EXOR
済み平文
(C)
EXOR済み
暗号文

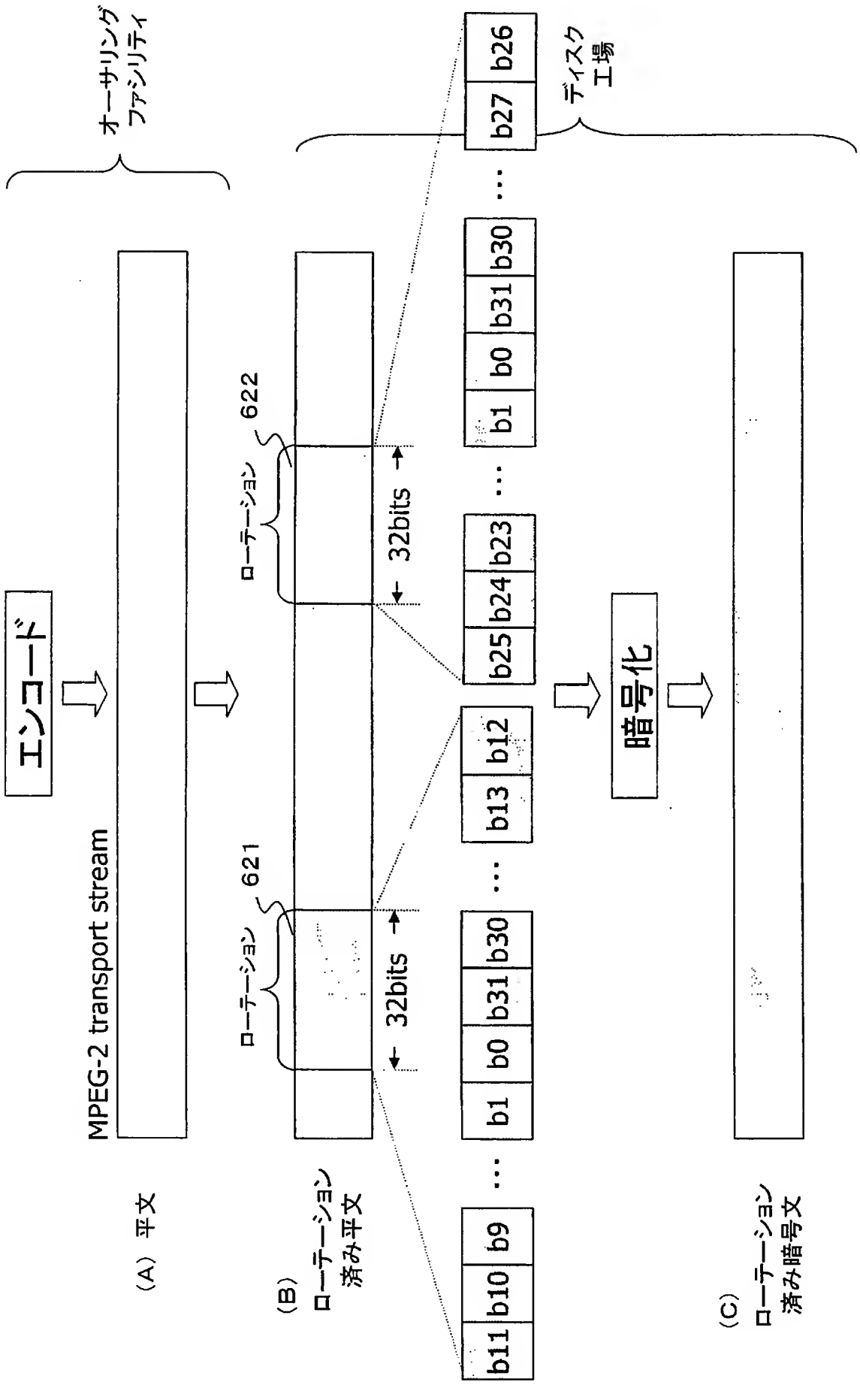
[図27]


オーサリング
ファシリティ
ディスク
工場
エンコード
MPEG-2 transport stream
(A) 平文
(B)
ローテーション
済み平文
(C)
ローテーション
済み暗号文
暗号化
611
612
32bits
32bits
b11 b10 b9 ... b1 b0 b31 b30 b13 b12
b25 b24 b23 ... b1 b0 b31 b30 b27 b26

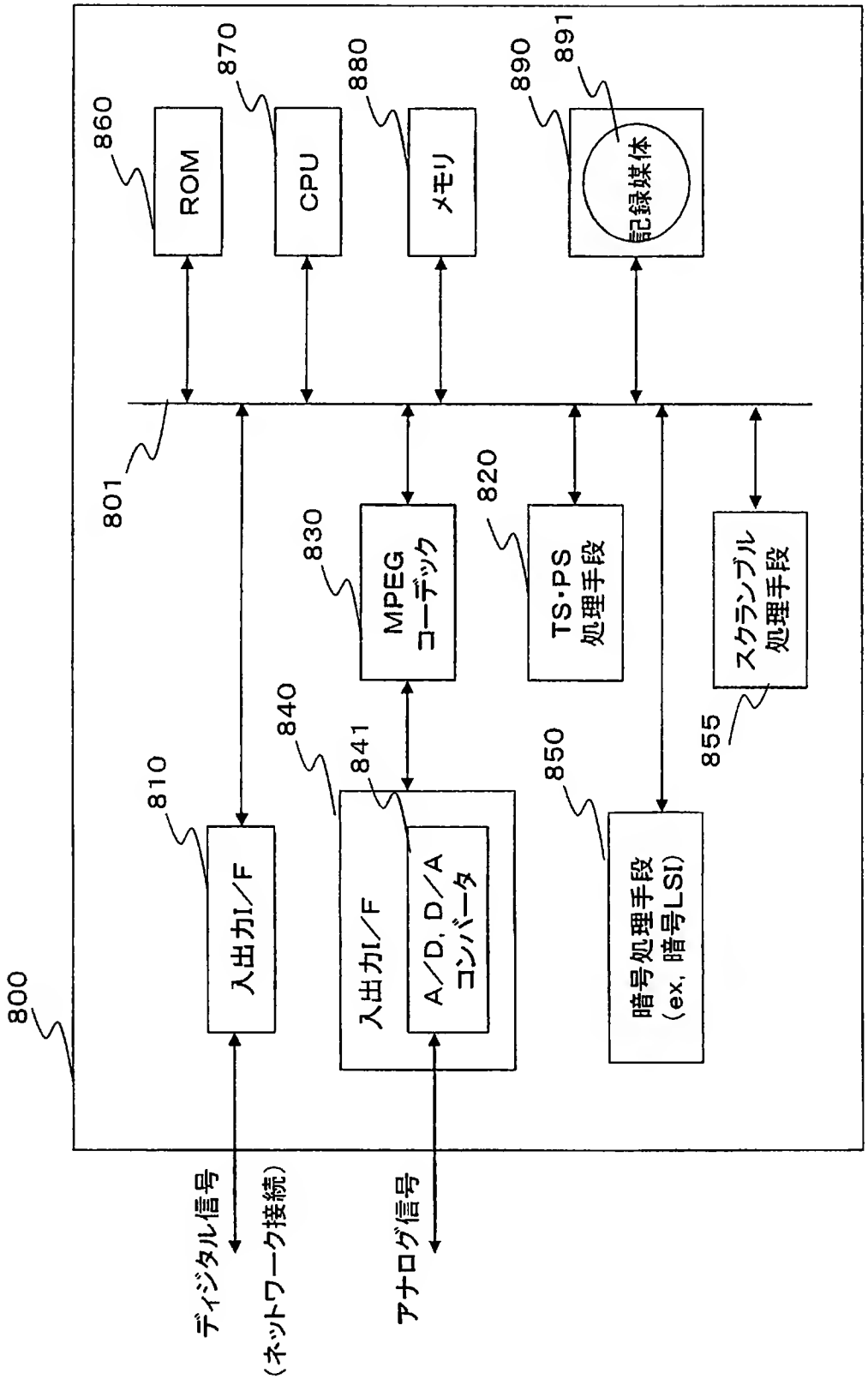
[図28]



[図29]


オーサリング
ファシリティ
エンコード
MPEG-2 transport stream
(A) 平文
ローテーション
621
622
32bits
(B)
ローテーション
済み平文
b11 b10 b9 ... b1 b0 b31 b30 b13 b12 b25 b24 b23 ... b1 b0 b31 b30 ... b27 b26
ディスク
工場
暗号化
(C)
ローテーション
済み暗号文

[図30]


800
801
810
入出力I／F
840
841
入出力I／F
A／D, D／A
コンバータ
850
暗号処理手段
(ex, 暗号LSI)
855
スクランブル
処理手段
820
TS・PS
処理手段
830
MPEG
コーデック
860
ROM
870
CPU
880
メモリ
890
891
記録媒体
ディジタル信号
(ネットワーク接続)
アナログ信号

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/020968

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/14(2006.01), ***G06F21/24***(2006.01), ***G09C1/00***(2006.01), ***G11B20/10***(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/14(2006.01), ***G06F21/24***(2006.01), ***G09C1/00***(2006.01), ***G11B20/10***(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 10-145773 A (Toshiba Corp.), 29 May, 1998 (29.05.98), Par. Nos. [0014] to [0016]; Figs. 2 to 4 & US 6021199 A	1,9,10,18, 19,27,28, 34-38 7,8,16,17, 25,26,33
X	JP 7-281596 A (International Business Machines Corp.), 27 October, 1995 (27.10.95), Par. Nos. [0017] to [0028]; Figs. 1 to 7 & US 5548648 A & EP 676876 A1 & GB 2288519 A	1-6,10-15, 19-24,28-32, 35-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 05 December, 2005 (05.12.05)	Date of mailing of the international search report 13 December, 2005 (13.12.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/020968

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-342246 A (Sony Corp.), 02 December, 2004 (02.12.04), Par. Nos. [0170] to [0193]; Figs. 18, 19 (Family: none)	7,8,16,17, 25,26,33
A	JP 9-270785 A (Fuji Xerox Co., Ltd.), 14 October, 1997 (14.10.97), Par. Nos. [0071] to [0074]; Figs. 1 to 7 & US 5995623 A	1,3-6,10, 12-15,19, 21-24,28-32, 35-38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/020968

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee..

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

<Concerning Unity of Invention>

The matter common to the inventions of claims 1-38 is that a scrambling of a content is carried out according to a scramble rule and the scramble rule and a scrambled content are recorded in a recording medium.

However, the international search has revealed that the common matter is not novel since it is disclosed in the documents below.

Document 1: JP 10-145773 A (Toshiba Corp.), 29 May, 1998, paragraphs [0014] to [0016], figures 2 to 4

Document 2: JP 7-281596 A (International Business Machines Corp.), 27 October 1995, paragraphs [0017] to [0028], figures 1 to 7.

Consequently, since the common matter makes no contribution over the prior art, the common matter cannot be a special technical feature within the meaning of PCT Rule 13.2, second sentence. Therefore there is no matter common to all the inventions of claims 1-38.

Hereinafter, whether or not the claims dependent on a claim group A (claims 1, 10, 19, 28, 35-38) satisfy the requirement of unity of invention will be examined.

The inventions of claim group B (claims 2, 11, 20) is an invention using an individual scramble rule for each content.

The invention of claim group C (claims 3, 12, 21, 29) is an invention using substitution in scrambling.

The invention of claim group D (claims 4, 13, 22, 30) is an invention using shuffle in scrambling.

The invention of claim group E (claims 5, 14, 23, 31) is an invention using exclusive-OR as scrambling.

The invention of claim group F (claims 6, 15, 24, 32) is an invention using rotation in scrambling.

The invention of claim group G (claims 7, 8, 16, 17, 25, 26, 33) is an invention in which encrypting is carried out in addition to scrambling.

The invention of claim group F (claims 9, 18, 27, 34) is an invention in which objective data is designated for scrambling.

In the inventions of claim groups C-F , they are related in the point that the specific scrambling is specified. However, they are not novel since their constitutions are disclosed in Document 2, paragraph [0017]. Consequently, the inventions of claim groups C-F do not share a common special technical feature and therefore do not satisfy the requirement of unity of invention.

Furthermore, the inventions of claim groups A-F cannot be considered to satisfy the requirement of unity of invention.

From above reasons, the international application is perceived to contain 8 inventions of claim groups A-F.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０２０９６８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　***H04L9/14*** (2006.01), ***G06F21/24*** (2006.01), ***G09C1/00*** (2006.01), ***G11B20/10*** (2006.01)

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　***H04L9/14*** (2006.01), ***G06F21/24*** (2006.01), ***G09C1/00*** (2006.01), ***G11B20/10*** (2006.01)

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 10-145773 A (株式会社東芝), 1998.05.29, 段落【0014】－【0016】, 図2-4 & US 6021199 A	1, 9, 10, 18, 19, 27, 28, 34-38
Y		7, 8, 16, 17, 25, 26, 33

☑ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０５．１２．２００５	１３．１２．２００５

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5S	3365
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	石田　信行 電話番号　０３－３５８１－１１０１　内線　３５４６		

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 7-281596 A（インターナショナル・ビジネス・マシーンズ・コーポレイション），1995.10.27，段落【0017】－【0028】，図1-7 & US 5548648 A & EP 676876 A1 & GB 2288519 A	1-6, 10-15, 19-24, 28-32, 35-38
Y	JP 2004-342246 A（ソニー株式会社）2004.12.02，段落【0170】－【0193】，図18,19（ファミリーなし）	7, 8, 16, 17, 25, 26, 33
A	JP 9-270785 A（富士ゼロックス株式会社）1997.10.14，段落【0071】－【0074】，図1-7 & US 5995623 A	1, 3-6, 10, 12-15, 19, 21-24, 28-32, 35-38

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２００５／０２０９６８

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。
特別ページ参照

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付を伴う異議申立てがなかった。

＜発明の単一性について＞

請求の範囲１－３８に係る発明の共通の事項は、スクランブルルールに従ってコンテンツに対するスクランブル処理を行い、前記スクランブルルールとスクランブルコンテンツを記録媒体に記録することである。

しかしながら、調査の結果、上記共通事項については、

文献１：ＪＰ　１０－１４５７７３　Ａ（株式会社東芝），１９９８．０５．２９，段落【００１４】－【００１６】，図２－４、及び、

文献２：ＪＰ　７－２８１５９６　Ａ（インターナショナル・ビジネス・マシーンズ・コーポレイション），１９９５．１０．２７，段落【００１７】－【００２８】，図１－７

に開示されているから、新規でないことが明らかとなった。

結果として、上記共通事項は先行技術の域を出ないから、ＰＣＴ規則１３．２の第２文の意味において、かかる共通事項は特別な技術的特徴ではないから、請求の範囲１－３８に係る発明全てに共通の事項はない。

以下、請求の範囲群Ａ（請求の範囲１，１０，１９，２８，３５－３８）に従属する各請求の範囲が発明の単一性の要件を満たしているか検討する。

請求の範囲群Ｂ（請求の範囲２，１１，２０）に係る発明は、コンテンツ毎に個別のスクランブルルールを用いるものである。

請求の範囲群Ｃ（請求の範囲３，１２，２１，２９）に係る発明は、スクランブル処理に置き換えを用いたものである。

請求の範囲群Ｄ（請求の範囲４，１３，２２，３０）に係る発明は、スクランブル処理にシャッフルを用いたものである。

請求の範囲群Ｅ（請求の範囲５，１４，２３，３１）に係る発明は、スクランブル処理として排他的論理和演算を用いたものである。

請求の範囲群Ｆ（請求の範囲６，１５，２４，３２）に係る発明は、スクランブル処理にローテーションを用いたものである。

請求の範囲群Ｇ（請求の範囲７，８，１６，１７，２５，２６，３３）に係る発明は、スクランブル処理に加えて暗号化処理を行うものである。

請求の範囲群Ｆ（請求の範囲９，１８，２７，３４）に係る発明は、スクランブル処理の対象データを指定するものである。

上記請求の範囲群Ｃ－Ｆについては、具体的なスクランブル処理を特定している点で関連があるが、これらの構成については文献２の段落【００１７】に開示されているから新規ではない。ゆえに請求の範囲群Ｃ－Ｆにかかる発明は、特別な技術的特徴を共有するものとはいえないから、発明の単一性の要件を満たさない。

また、上記請求の範囲Ａ－Ｆに係る発明が発明の単一性の要件を満たすものとも認められない。

以上の理由から、本国際出願の発明は上記請求の範囲群Ａ－Ｆの８個と認められる。